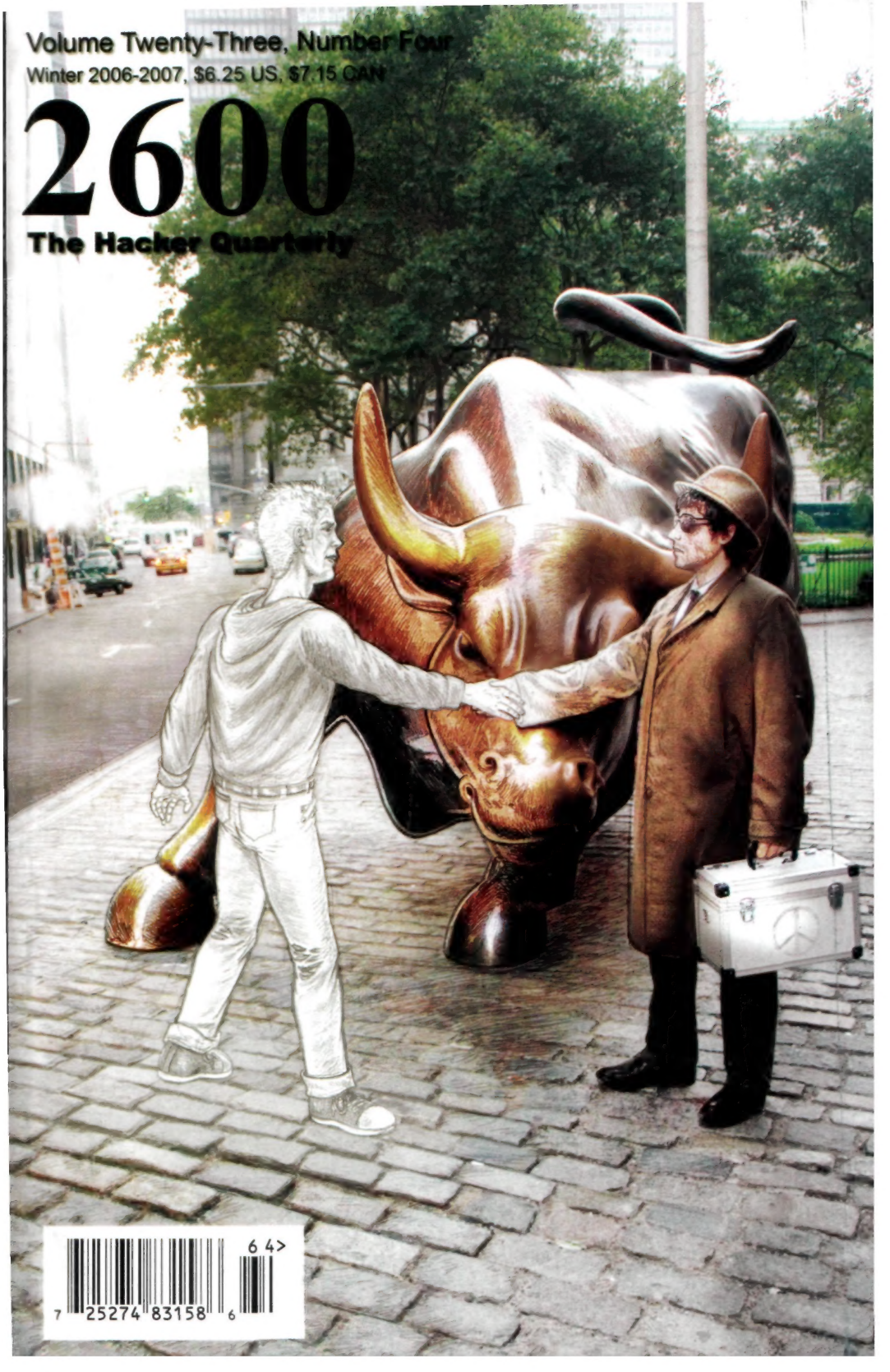

We Trip The Light
FANTASTIC

Volume Twenty-Three, Number Four
Winter 2006-2007, $6.25 US, $7.15 CAN

2600

The Hacker Quarterly



64>
7 25274 83158 6

Payphones of the World

Albania. A friendly looking orange phone which only takes cards. Found in **Tirana.**

Photo by Christian Smith

Turkey. This is a payphone booth in a small tow by the Aegean Sea near **Assos.** It takes credit card and phone cards while a light switch conveniently hangs from the ceiling.

Photo by John Shramk

Denmark. An old coin model. Taken outside one of the main train stations in **Copenhagen.**

Photo by rinjava

Japan. Old and big, yet it does it all. Seen in th city of **Kin** on the island of Okinawa.

Photo by Brian McIntos

Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)

EDUCATION

"It has become appallingly obvious that our technology has exceeded our humanity." - Albert Einstein

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover
Frederic Guimont, Dabu Ch'wald

Office Manager
Tampruf

Writers: Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, Redbird, David Ruderman, Screamer Chaotix, Sephail, Seraf, Silent Switchman, StankDawg, Mr. Upsetter

Webmasters: Juintz, Kerry

Network Operations: css

Quality Degradation: mlc

Broadcast Coordinators: Juintz, thal

IRC Admins: koz, sj, beave, carton, r0d3nt, shardy

Inspirational Music: Ride, The Frank & Walters, Focus, Harry Gregson-Williams, Jean Leloup, Jah Wobble, Asian Dub Foundation, Nilsson, Flotsam & Jetsam (original)

Shout Outs: Steve Rambam, Rick Dakan, Mitch Altman, Mike Aiello, DerEngel, No Starch, Prometheus, Stevens Institute, Montreal 2600

2600 *(ISSN 0749-3851, USPS # 003-176), Winter 2006-2007, Volume 23 Issue 4, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices. Subscription rates in the U.S. $20 for one year.*
POSTMASTER: Send address changes to 2600, P.O. Box 752, Middle Island, NY 11953-0752.

YEARLY SUBSCRIPTION:
U.S. and Canada - $20 individual, $50 corporate (U.S. Funds)
Overseas - $30 individual, $65 corporate

Back issues available for 1984-2005 at $20 per year, $26 per year overseas
Individual issues available from 1988 on at $5.00 each, $6.50 each overseas

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 USA (subs@2600.com)

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099 USA (letters@2600.com, articles@2600.com)

***2600* Office Line: +1 631 751 2600**
***2600* Fax Line: +1 631 474 2677**

Transition

It's been a sobering period recently in the world of publishing. All around us we hear gloomy tidings of the condition of the industry and its prospects for the future. We've been saddened to witness the demise of some other printed publications as their expenses became too much for them to bear. The alternative voices always seem to be the first ones affected while those immersed in the world of advertising and all things commercial seem to weather the storms and survive the challenges. Money in abundance tends to make such things possible.

Our mission has always been to provide information and provocative thought without being tainted by the wanton commercialization that afflicts so many. As we come to the end of our 23rd year, we're both amazed that we were able to pull it off and confident that we can continue to fulfill this purpose in the years ahead. We are unique in the publishing world and so is our audience. And since our subject matter is mostly about individuality, challenging the status quo, and figuring out the exception to the rules, this all ties together rather nicely.

But we too have faced some daunting challenges in recent months and they have resulted in some painful decisions for us. Despite our unique position, we still feel the affects of trends and right now the trend is a downturn for anyone in the publishing business. As mentioned, this mostly affects the small publishers since they don't have much to fall back on. Large publishers can jack up advertising rates, lay off staff, and even merge with other publications without missing a beat. To them it's merely a business decision. But for noncommercial publishers it's a bit trickier. Distributors only pay publishers for issues sold. The rest are destroyed at the publishers' expense. The bigger bookstores and newsstands can often thrive by providing alternatives to whatever is not selling at the moment, even if that means cutting back on books, magazines, and newspapers. In that section of the industry, the independent retailer feels it the hardest. In a parallel to the small publishers' problems, small bookstores all over the country have felt the pressure and are increasingly falling victim to the huge chains which now dominate. It's a sad situation, one which we see repeated in so many different ways in our society.

We have a great advantage in that our audience is already clued in to a great deal of this and understands the value of a printed publication such as ours. Ironically, the very people who understand technology and the Internet on a level far exceeding the norm are the same people who still value ink on a page and the power of the printed word, something that is mostly lost in the world of the net. So while we certainly feel the affects of what has been happening in the world of publishing, we think we'll be able to weather the storm, assuming that's what our readers want.

In the end that's really what it's all about. If we cease being relevant to our readers, our existence comes to a conclusion. This is how it should be. In fact, we believe there would be a lot less commercial publications for that very reason if they weren't doing so well on the advertising front. We don't have that luxury nor do we want it. A publication should exist entirely to serve its readers. We hope we continue to achieve that goal. Your vote determines whether or not we do.

We also hope our modest price increase on the newsstand won't be a hardship. It's our first one in quite a while and we avoided it as long as we could. We can't ignore the rising costs around us and the increasing challenges of the

marketplace. However, we have also moved forward with a planned increase in pages and as of this issue we have four more of them. We have not changed the subscription price and it remains what it has been for more than 15 years. We've also lowered the newsstand price in Canada to reflect more accurately the currency conversion there.

This is only one step we've been forced to take in order to deal with all of the challenges thrown our way. We have had to change printers for the first time in 20 years, a move we resisted when we could afford to. It's a very sad fact but sometimes a business decision has to supersede loyalty and tradition. In this case, the only alternative would have been cutbacks and price increases that in our opinion would have been unfair to our readers.

From our perspective it certainly seems as if an undue amount of the burden comes to rest on publishers which in turn causes so many of them to cease what they do. Over the years we've seen a large number of distributors collect money from bookstores and fail to pay the publishers who sent them the magazines in the first place. The distributors then declare bankruptcy and the publishers never get paid. This scenario seems to play out on a yearly basis somewhere and each time it does, a few more independent voices are silenced for good. We've also seen many chain outlets go under and fail to pay their debts, causing the same trickle-down effect. In addition to all of this, we must frequently accept terms and conditions that go against common sense and are seemingly designed to put the publisher at a disadvantage.

A good example of this is something known as "shrink policy" in Barnes and Noble, the largest bookstore chain in the United States. Shrink is the industry term for issues that cannot be accounted for after being delivered to the store. This policy actually forces publishers to pay a significant portion for these issues, as if they were somehow responsible for them. The thinking - as far as we can tell - is that if copies of your publication are being shoplifted, it's the fault of your readers and therefore your responsibility. But this doesn't take into account a number of things. Issues can get lost in a store for a number of reasons such as misfiling or accidental destruction. They can also be stolen by store employees themselves. (Industry surveys have found that more than half of store thefts come from people who work in the stores.) In extreme cases, anyone (employee or customer) can decide they don't like us and pitch all of our issues into the trash.

In the past, a major cause of shrink was the failure of the cashier to properly enter the sales data into the computer. Sometimes the bar code wouldn't scan properly and a generic sale that didn't have the publication's name would be processed instead. This meant that there was no actual record of the magazine being sold even though the store collected the money. We're told that such a scenario is now impossible. We find that extremely hard to believe.

The main problem, though, is that this policy is horribly unfair to publishers. By this logic, if we were to buy a book at Barnes and Noble and someone stole it from us afterwards, we could hold the bookstore responsible. It goes against all common sense. The only way publishers should be held liable for missing issues is if they somehow have the power to do something about it. We've offered to send in our own security people to various stores to stand guard over copies of *2600* to ensure that none disappeared. (We naturally would have to watch them after the store closed as well to prevent employee theft.) No store has yet agreed to this.

Don't get us wrong - Barnes and Noble has been a great resource in getting our magazine out to the public and we're thrilled to be on their shelves. But we're also compelled to speak out when something doesn't seem quite right, whether it's an issue like this or a security hole in a computer or phone system. It's what we do and it's what continues to make us unique. And, in this case, not saying something could help this policy to become the norm in all bookstores, something which once again would hurt the small publishers far more than the big ones.

All in all, we think we're going to be in pretty good shape once we get through the woods. In the next issue we're planning on including a survey form for subscribers so we can all plan for the future and learn from the past. We look forward to embarking on more fun projects in the future involving publishing, HOPE conferences, films, radio, new technology, etc. And, of course, controversy. We hope you all continue to be a part of it.

Mobile Devices - Current and Future Security Threats

by Toby Zimmerer

This article will focus on a system that many people utilize every day. Yet they are oblivious to the power of the threat that they are exposed to. That system is your mobile phone. The advent of smart phones and PDAs has spawned a new security hole that the majority of people completely ignore. Most mobile phones can access the Internet and have Bluetooth communication systems for linking other devices without the use of cables. Additionally, smart phones are utilizing Linux and Windows operating systems and have the processing capabilities of a small computer. Since these devices do not have a built in firewall and provide multiple open communication channels, it becomes perfectly clear that mobile phones pose a prime target for attacks.

Mobile Devices and Operating Systems

Smart phones are currently using two operating systems (Symbian and Windows Mobile 5) that are customized to each cellular provider's mobile device. Symbian (http://www.symbian.com/) is a lightweight Linux operating system that is bundled with a number of applications that can allow a user to work on the road without the use of a laptop. Microsoft has taken their lightweight Windows OS that was originally developed for the iPaq and into the cellular provider market by developing Windows Mobile 5 (http://www.microsoft.com/windowsmo➥bile). Microsoft offers a complement of applications to allow a user to work remotely without the use of a laptop.

For those of you not familiar with smart phones, I would suggest looking at the websites for Symbian and Microsoft Mobile in order to see the mobile devices that are currently supported. As I mentioned earlier, smart phones have the processing capabilities of a small computer. These phones are normally equipped with 64MB to 128MB of memory and can be expanded up to 2GB of additional memory by adding a mini SD memory card to the phone. Some smart phones have integrated keyboards and touch screens that allow you to quickly navigate through menus and enter information. I own a Nokia 9300 that flips open to give the user access to a 1" x 4" high resolution LCD, a 66 button keyboard, and a thumb mouse.

Open Communication Channels

Mobile service providers have expanded their services to provide users with greater access in information through their mobile phones. People in Europe and Japan have been using their mobile phones for web access, messaging, and purchasing goods directly from their mobile phones long before the U.S. market started to offer these services. Mobile phones can retrieve an IP address from their mobile service provider, which provides full access to the Internet to transmit http, SMTP, SSH, telnet, and other TCP/UDP functions.

Most devices are now equipped with Bluetooth to allow the user to connect to their laptops, wireless headsets, or other mobile devices. Bluetooth has a transmit radius of approximately 30 feet and can be configured to allow other devices to find or "discover" the host device. Open Bluetooth channels broadcast a lot of information, including the MAC address, device name, and device model. I saw a demonstration at the Interop show in Las Vegas this year where the vendor was listing all of the Bluetooth connections that were currently open near their booth. On average, there were 60 open Bluetooth connections near the vendor's booth and they were able to retrieve the device name and model device. As a test, I switched on the Bluetooth connection on my phone, disabled the discover feature, and my device was detected.

If you are interested in performing some Bluetooth vulnerability scanning, I would recommend checking out BTScanner by PenTest (http://www.➥pentest.co.uk/), which runs on a desktop system, or Blooover (http://trifinite.org/trifinite_stuff_blooover.➥html), which runs on your handheld device.

Current and Future Mobile Threats

Mobile device viruses began to show up in 2004 with the release of the Cabir virus. Since then, the number of viruses has grown exponentially, which has resulted in both financial and hardware loss. The Skulls and Onehop viruses are designed to completely disable the mobile handset, whereas the CommWarrior virus will start to transmit SMS messages to everyone in your address book, resulting in additional costs on your phone bill.

These viruses currently propagate through two mediums: SMS and Bluetooth. The CommWarrior virus shows up as an SMS message with an SIS attachment. If the user activates the attachment, the mobile phone will become infected. Bluetooth viruses, such as Cabir, broadcast a message with an attachment to all Bluetooth devices in range. Once again, if the user activates the attachment, the phone will be infected.

As I had mentioned earlier, mobile devices are now retrieving IP addresses and run compact oper-

ating systems to provide the user with all the features and functions of a desktop system on their mobile devices. These systems do contain software flaws and holes that will eventually get exploited through the open Internet channel on the devices, leaving the users vulnerable to attacks. As of March, the first Java2 ME viruses started to appear. Sooner or later, viruses will start to propagate to mobile devices over the Internet.

Defending Against Mobile Threats

Currently some software companies are offering anti-virus and firewalls for mobile devices. I would recommend doing some research on the different vendors to see which companies support the broadest range of mobile devices and operating systems. I know one company has been designing mobile AV/firewall solutions for a number of years and has a pretty large distribution throughout the world with a number of mobile service providers. I will let you make your own decision on which route to go. Additionally, I would scan your open Bluetooth connections to see how many open connections you have. Finally, and most importantly, educate yourself and those around you. Most of the current mobile viruses can be thwarted by deleting the attachment or not opening it at all.

Mobile devices are the next vulnerable resource on the market today and will eventually be targeted by viruses that spread across multiple communication channels. As the complexity, features, and processing power of the mobile devices increase, they will provide a prime avenue for malware to exploit. By protecting your mobile devices with anti-virus and firewalls, as well as disabling unnecessary services such as Bluetooth, you can protect your network and yourself from current and future threats.

FirstClass Hacking

by Cristian

The idea to write this article came from reading this magazine for a while. I noticed that lots of people were writing in about the (in)security of the place they were studying in. Having read all these articles/letters very thoroughly, I decided to look into the security in the place I go to study. I go to an English CEGEP, which is basically a hybrid of year 12 in school and the first couple of years of university. When you first enroll into the CEGEP you are given a student ID card which has a magnetic strip, your picture, and your student ID number. The magnetic strip contains the SID number too, as well as a "charge" of $4.00 CDN in order to be able to print in certain computer labs throughout the campus. Using a combination of methods, we will obtain both the SID number and the corresponding password, thereby showing how vulnerable this system really is. This of course should be taken as an educational guide and not to be used for your own gain.

The Student ID Number

The student ID number is used to log into your FirstClass (www.firstclass.com) account, which is the piece of software used all over the campus for pretty much any class related tasks. We use FirstClass for everything, from viewing our assessments to communicating with the teachers. Teachers, on the other hand, use it to actually put our grades into the system, calculate class averages, etc. We also use this SID to log into our "For Students Only" section where it shows us all our grade history, our current schedule for the semester, our CRC score (a sort of GPA), and a couple of other features. It is also used for the OmniVox service. We use this web-based service to view our grades with more details (class averages, graphs, etc.), pay our student fees for the semester, get a tax receipt for being a student, or change our home address and phone number. Lastly, we use the SID to be able to make our schedules a couple of weeks prior to the semester starting. The system is phone based, so you simply call and follow the instructions given to log in.

Vulnerabilities

The Birthdate

There are various vulnerabilities in the system, so I will go in the order I discovered them. Upon your first entry to the college, they tell you that your pin (to be used in FirstClass, "For Students Only," OmniVox, and course registration system) is your birthday, in the form of DDMMYY, including the 0s if the day or month has it. Social engineering, anyone? If you are able to engage a conversation with someone, it should be quite easy to obtain their date of birth. Even worse, the CEGEP I attend is chock full of people who use the infamous MySpace.com website, so even if they don't tell you their date of birth, asking them for their MySpace page is another option. Simply looking at their description may reveal this bit of information or, if not, look at the comments other people leave. There might be messages wishing a happy birthday and then you can deduce the date of birth of the person.

The Student ID Number

Knowing the birth date is only half the information we need since the SID number is the next important part. The SID number is seven digits and has the format YYXXXXX, where YY is the year you first enrolled into the CEGEP and the remaining Xs are

generated at random (to my knowledge). Finding this number is quite easy and there are actually various ways to find it.

For one thing, everyone must carry their SID card inside the campus or they will be kicked out by the security guards as well as fined $50 CDN. Again, social engineering can be applied here and simply asking someone you know to show you their ID card to see how goofy they look in their picture will give you full access to the SID, so memorizing it shouldn't be that big of a problem.

Another way to find it is by looking in the recycling bins. The students over here print like crazy, and in all essays/lab reports, etc. you must provide your name and SID number so the teacher can then input the grade into the FirstClass system. Usually you can find old lab reports or pages that have mistakes in them with the student's name and SID number fully viewable in the page's header.

The third way to find it is directly via the FirstClass system. Upon logging into the system, you will be greeted by the "Desktop" of your FirstClass account which has links to your mailbox, address book, calendar, current semester registration process, conferences, uploaded files, help, news, and student body forum. To your left you have the FirstClass menu system, which has links to logout, who's online in the system at the time, instant message menu, preferences, and, more importantly, the directory.

The directory is a search engine which takes in a name (or part of a name) and searches matches across the student body and the faculty/teachers. Now if you search for someone (let's say Smith), it will return anyone with the surname Smith in it (both student and teacher). Once the matches appear, it will provide links to their FirstClass shared files folders. For teachers, this is quite useful since they can provide class notes, PowerPoint presentations, etc. for everyone to download. For students, well, I haven't met anyone that actually uses that service yet. The important part here is the list of links that is provided when a match is found. If the person is a teacher (let's say we found a teacher named John Smith), then pointing to the link will provide an address such as the following in the status bar of your browser:

```
http://firstclass.COLLEGENAMEHERE.qc.ca/
➥Login/~SMITHJ/
```

There isn't very much to work with in that link, right? Well, now let's say that the list of matches is greater than a single result and that at least one of the matches is a student. If you point to that link, the status bar will display the following address:

```
http://firstclass.COLLEGENAMEHERE.qc.ca/
➥~YYXXXXX/
```

Recognize something there? Lo and behold, the link provides the SID number of the student we searched for - without even knowing the student in real life.

It is also worth noting that when you change your password for the "For Students Only" page, it only applies to that individual system. Your birth date will still be the password for the Omnivox, FirstClass, and phone registration systems. Even worse, in order to actually change these passwords, you cannot do it via the actual system. You must physically go to the IT Administrator's office (which very few students know how to find) with two pieces of ID in order to change them. Making it this hard to change a password is very unreasonable. Students are lazy and they have work to do. They aren't going to go through the trouble of finding out where the office is just to change their password. They'd rather just keep it as it is and just forget about the potential consequences that could happen.

Combining these two pieces of information gives us literally access to anything related to that particular student. You are able to change their address, their phone number, and once schedule-making time comes, you can easily delete all his/her courses and have him/her be charged $50 CDN for registering late, as well as leaving an empty spot in the classes he/she took (which, if you need that course, can be taken by you).

It's very surprising that they have such an elaborate system for managing your stay at the CEGEP, but it can be very easily bypassed with a few simple clicks and a little bit of social engineering. Even worse is the terrible method that they have to perform a simple task like changing a password. If you ask me, it's a very small price to pay for your privacy.

Network Administrators: Rules Rationale

by The Piano Guy

When I wrote my article "Network Administrators: Why We Make Harsh Rules" (22:4), my purpose was to explain what seemed like, to some, capricious rules that some network administrators hand down. I did it in reaction to a student (Luke) who ran afoul of the rules and was being taunted by a stupid and unprofessional network administrator. I wrote the article with a bit of fear and trepidation. Though I didn't think this was what I was doing in reality, I felt like I might be perceived as "the other side," rather like Hamas writing into the *Jewish News* to explain their actions.

The next issue had an attack letter implying that my article was stupid and that I should just stop whining and "do my job." The editor of *2600* chal-

lenged the letter's author, explained why I wrote it, and why they published it. Frankly, I thought a former employee of ours sent in the letter. I write like I talk, he reads and writes for this magazine, and he's certainly smart enough to figure out that I authored the original article. If my hunch is right, the man is stunningly brilliant with computers. He certainly had more technical skills than most, including me. He didn't, however, work in my department, didn't like me, and I don't know why he was fired, other than to know that I had nothing to do with it.

Three months later, kaigeX wrote a thoughtful rebuttal article. Though he took me to task, he mostly agreed with more than half of the rules that the other system administrator handed down for me to enforce. A well-reasoned response deserves a well-reasoned rebuttal. To clear the air, I'm going to review the points he made about the points in my article. If you can't follow all of this, do remember that *2600* does sell back issues.

His interpretation of my rules was in essence "we make harsh rules to make our lives easier and/or to protect ourselves." He didn't think this was legitimate. I don't exactly agree with his interpretation. If I had to boil this down, I would say that we make harsh rules to keep the network usable for all people so they can get their jobs done and to protect the employer (owner of the network) from massive expenses in repairs and/or from legal action from outside entities. Do note that I'm not offering "so they can manage their personal lives better (i.e., checking your Gmail or doing your banking online)." The purpose for providing computers in the first place is to facilitate work. That's why the owners pay for the network, and for me to run it. When put that way, the emphasis changes.

He didn't think that our library computers were secured at all, thus unfit for use by him. I don't think that's what I said, and I'm certain that's not what I meant. They are secured. They are on a different network (good question to ask, kaigeX). They aren't as restricted and are perfectly useful for web mail when employees are on break.

He thinks the "hard rules" cause a loss of productivity. The opposite is true. So is my emphasis. In fact, it is my job to find ways to improve processes to make people's work easier. Sometimes that means writing a Crystal Report or some SQL code. Sometimes that means buying, installing, and supporting specialized software on a user's computer. And yes, sometimes that means opening up services on the network just for a certain department. Whatever it is, it is my job to serve.

Now, if I'm constantly chasing down viruses and/or spyware, dealing with user complaints about how slow the network is, or spending time in depositions answering questions about copyright infringement by one of my users, I won't have time to find new efficiencies, let alone implement them.

The comment I made that bothered kaigeX the most was that if someone broke a rule and it didn't cause a problem, then we probably weren't going to even notice. He somehow makes the leap that we expect people are going to have to break the rules to get their jobs done, so we set the expectations high knowing the people aren't going to follow them. Maybe kaigeX has never had to deal with a legal department. Surely he can use some clarification about how and why I do things. The purpose of the network is so people can get their work done. Everything we do derives from that basic premise. No one ever has to break a rule to get his or her job done - period. This is so true that if something comes up requiring a user to break a rule to get their job done, we either find a different way or change the rule, which covers Number 9 (no hacking). This also covers Number 2 (no one connects devices without permission) because if they need it for their job they have permission. It covers Number 3 (no one installs their own software) and Number 8 (no copyright infringement). If they need it, we buy it for them so we're legal, and support it. Unlike where kaigeX has been, we are 100 percent legally licensed for everything. In fact, that was the main reason why my predecessor was fired - he didn't see a need to be 100 percent legal. And peripherally, it covers Number 5 (no chat software). We encourage people to use their mail clients as if they are chat clients. It's almost as fast and this leaves an audit trail for them to refer to later (in their Sent Items).

Further, we try to strike a balance between being a police state and being open to lawsuits. We could strictly enforce Number 1 (business use only) and Number 10 (no expectation of privacy), but that would be highly stupid and counterproductive. It would take a lot of time and resources, and it would irk people to no end. However, let's say that someone does something really stupid, like surf for kiddy porn while at work (which happened where I was employed in 1991). We need legal grounds to look for it if we suspect something, or handle it if we find it by accident. We also need legal protection so we can terminate this employee without being sued by them. In this extreme example, a law was broken. So heaven forbid it if ever happens to us, we would need legal protection to turn in evidence against them to the police.

Onto other points. KaigeX's disagreement with my Number 4 (no outside email clients) goes against productivity for work and also puts my network at risk. It also causes political problems in the workplace. My brilliant former coworker (BFC) is more than smart enough not to bring in viruses via his outside email usage, but his ignorant department director (IDD), two management levels above him, is computer stupid. If BFC has the "right" to check his email, how am I going to deny this to IDD? If I do deny it, what's to prevent IDD from demanding that BFC set this up for him, even if I've said not to? Nothing. Also, if BFC sets it up, I have no way to block attachments from coming in for IDD to open up (a workaround that kaigeX suggested), taking my

etwork and the workstations on it to DOA.

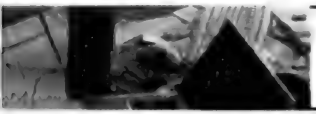
Remember folks, I didn't write these rules. I was anded these rules to enforce, and I do. I also have o follow them, if not for safety reasons, then for olitical reasons. If I broke a rule I am supposed to nforce and did serious damage to the network as result, the person they hired to replace me would e the one to clean it up. Lastly, I've always held the erspective that one thing worse than a hypocrite is eing one.

More or less, kaigeX agreed with every other oint I made. He didn't necessarily like that he had o agree with me, but apparently it didn't occur to im that I don't necessarily like to have to take a osition either.

Lastly, kaigeX made one blatant factual error. He feels that I am at risk because of my Win2K workstations not getting security patches. Go to http://support.microsoft.com/lifecycle/?p1=7274 and http://support.microsoft.com/gp/lifecycle (unless Micro$oft changes the pages). They make clear that security patches are provided through 7/13/2010. By that date all of my 2000 machines will be long retired, and my employer will probably have a combination of XP Professional and whatever is newer than that for the desktop.

Shouts out to kaigeX (for a reasoned rebuttal) and the anonymous network administrator who both set these rules we're discussing and taught me a lot over the last years of working with him.

Wi-Fi Hunting:



Basic Tools and Techniques

by Rick Davis

From war-walking to war-driving the art of finding wireless connections has become a game for a new mix of computer users. Finding new techniques calls upon knowledge in antenna design and signal theory along with various aspects of computer hardware and software. Sometimes though these higher level techniques are not reasonably used and for many that have not had experience with them simpler methods need to be employed. With this in mind the following will explore some of the best methods, in terms of cost and ease, to seek out available wireless connections.

Get Your Gear - Basic Hardware

At the most basic level you need only a laptop or other device that can connect to wireless connections. I recommend a laptop so that you can use some advanced software and several applications simultaneously (see below). Also, a wi-fi finder is very useful and will make your search quicker, more productive, and much more incognito. These devices can be found in any major electronics store and range from $10 to $30. They usually have a few LED lights packaged inside a casing about the size of any other pocket electronic device. Although they all have different features, they all do about the same thing which is indicate any time a wireless connection is detected by lighting a light. Some models can also tell you the strength and type of signal but I prefer to use my software for that and save the extra money.

More Gear - Basic Software

Get familiar with your OS's built in function to connect wirelessly because that can be used in many cases and is usually a quick way to connect. For example, Windows XP users can simply right-click the icon in the system tray to open the connections window which will display any available networks.

In addition, Network Stumbler provides a gold mine of information and in many cases may be the only other application you need. What this does is gather information from any signal it finds such as SSID, signal strength, security, and encryption being utilized along with many other features. There are many ways to keep the basic operating system from finding a connection (such as not broadcasting your SSID) however if there is a signal Network Stumbler will notify you.

It's also worth noting that some of these programs seek connections actively while others seek passively and depending on your situation this can make a difference. Actively means that your program is sending information in order to get a response and collect data, while a passive program transmits nothing and only collects what is passing by. Passive programs can take much more time to locate connections and will usually not detect all available data however it will also not get you logged by any software or data and connection logs.

Are You Secure?

Connecting at random locations, especially schools and cafes, will open your computer to possible attacks by many people. Most will be just

harmless people who click on anything their system may find although some will be far more advanced and able to access your system if you're not protected. Luckily, some basic steps can be taken to make you less of a target and not worth the trouble among a group of others.

First, firewalls are a must and one from a third party is a good idea to add an extra layer to whatever your operating system may already have running. Make sure you have them set to ask for authorization for any connection or data transfer and that you have security logs running. Next, make sure you have all the updates for any operating system you use as well as any software that connects to the Internet or is linked to the OS (such as chat programs). Finally, it should go without saying but make sure you have a fully updated anti-virus running.

Let's Get Started!

Option 1 - Locating a connection within a specific area: Whether it's a city block where you have lunch or your school campus, this is a great way to quickly map out connections without drawing any attention. You can either make a rough drawing of the area you want to search or you can take a notepad to quickly note where you found a signal to look into later. In either case just take your wi-fi finder and start wandering around. If you are not worried about being seen, or just don't think anyone will care, you can cover the whole area at once. Otherwise make sure you remember where you have been so your next trip will not duplicate your progress. Again, there are two options for a thorough search. Either walk around in a pattern so that all the searchable area is covered or just circle buildings or open areas where you would want to connect or expect to see a connection.

If you want to find everything available you should really walk through the search in a logical progression. On the other hand if your needs are more legitimate you may want to narrow your search to places where you can plug something in to charge or have a bathroom or soda machine nearby.

Option 2 - Always on the hunt: In this case you just want to keep a note of any connection you come across in regular travels or where you have no specific target in mind. If you're driving or walking you can easily clip your wi-fi finder on your belt or car visor and make a note when it goes off. On the other hand if you have a reasonable battery or are taking a short trip you can keep your laptop running in a backpack, carrying case, or even folded under your arm.

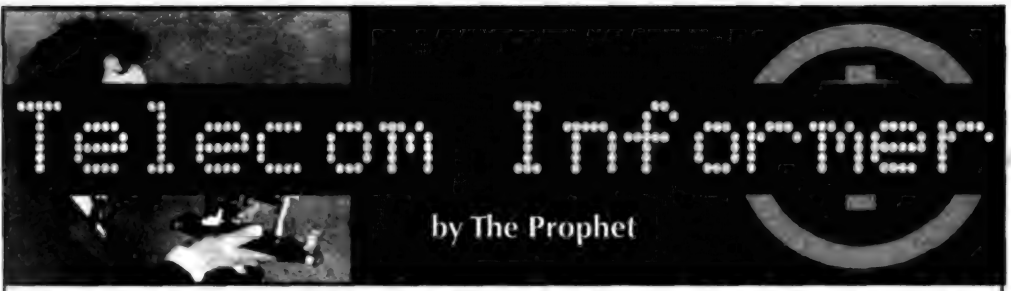
This can get somewhat cumbersome after a while although once you go through an area you can probably skip it for a few months. And of course while you are in an area where you know you will not connect, you can either power down your gear or completely ignore it.

Signal Found - Let Me In!

Now that you know where the signals are it's time to connect. The easiest method will be for an unsecured access point in which case you can click connect and you're online. Sometimes you can find a signal but cannot connect because you need some information and this is where your software comes in. Network Stumbler will give you the SSID of any connection and sometimes a router is set for open access and is just not broadcasting its ID. So all you need to do is manually enter it and, once again, you're online. Now the final piece of data from the Stumbler is the type of router you have accessed. Connecting to anything other than an unsecured access point is beyond the scope of this article. Whatever you might want to do however will require information on the type of router.

Closing Tips

Keep in mind that others have probably needed to connect in areas you're interested in as well. Don't be afraid to ask anyone nearby if they know of an access point. Also, at a school campus or office building you can always ask security or any computer technician. You may find out some great information plus if you are really only looking for legitimate access they will be able to warn you about anything that is off limits.



Hello, and greetings from the Central Office! At least I think it's the central office. Unfortunately, I was already halfway to Japan when the sushi hit the fan. After I got through running fiber to the igloo in Adak, my employer sent me here to Tokyo. I don't read Japanese, but my hosts assured me that central offices here are always clean, the vending machines are well-stocked, and the toilet seats are supposed to be heated. Unfortunately, they also assured me that when I'm through with my work, I really do have to go home.

When I haven't been either working or buying used schoolgirls' panties out of the vending machine at Love Merci Akihabara (it's on the second floor), I have been marveling at the mobile phones here. Everywhere in Japan, you'll find people texting, browsing the web, and taking pictures. They rarely talk on them, though; it's considered rude in most public places. Don't answer your "keitai" (the Japanese word for mobile phone) on a train, or you might find yourself at the wrong end of a samurai sword!

There are three major wireless service providers in Tokyo: SoftBank (formerly Vodafone), Kddi (marketed as "Au"), and NTT (marketed as DoCoMo). All offer true 3G data networks, although DoCoMo and SoftBank use UMTS (the same data technology available from Cingular in a few U.S. markets), and Au runs CDMA 1xEV-DO (available nationwide in the U.S. from Verizon and Sprint). GSM is considered obsolete in Japan and is not operated by any Japanese carrier.

Although Japan shares certain mobile phone technologies with the U.S., only Japanese phones can use Japanese mobile networks. This is because UMTS is used by SoftBank and DoCoMo for both voice and data, rather than using UMTS for data and GSM for voice as Cingular does. Additionally, different frequencies are used by these carriers than Cingular uses in the U.S. While Au uses the same CDMA technology operated by Verizon, Sprint, Alltel, US Cellular, and numerous other U.S. carriers, the transmit and receive frequencies are - for some reason - the exact opposite of those used in the U.S.

Global roaming is available to Japanese travelers using the GSM standard on all three carriers, and the CDMA standard using Au. However, this requires a special phone, and roaming rates are very high (for example, domestic calls in the U.S. are about US$1.00 per minute while roaming with a Japanese phone). This probably explains why so few Japanese phones offer global roaming; Au, for example, currently only offers one such phone.

Everything in this country is more complicated than it needs to be, and mobile phone plans are no exception. There is a dizzying array of plans, with only one common theme: they're absurdly expensive by U.S. standards. A typical plan (using Au as an example) costs about $40 per month, including just 60 minutes of calling. No free nights and weekends, no free long distance, and certainly no free mobile-mobile calling. But your unused minutes do roll over. The extras always cost extra; add another $40 for unlimited wireless data (to the handset only - tethering is not allowed). Wireless data includes unlimited email but not text messaging; that's another two cents per message sent.

Mobile phones have so many features, you might confuse them for a computer. In addition to the text messaging, email, web browsing, and picture mail capabilities available on most wireless phones in the U.S., Japanese mobile phones consider some pretty unusual things to be standard equipment. For example, no self-respecting Japanese handset would be caught dead without a Japanese-English dictionary built in. 50MB of RAM is standard equipment for a keitai, along with an FM radio, streaming media capability, GPS navigation, and a 2.4

megapixel camera.

You can use a mobile phone for all sorts of unexpected purposes in Japan, or potentially for playing all sorts of unexpected pranks. Consider the lowly cell phone camera. Apart from surreptitiously taking pictures of schoolgirls on trains (not that I'd ever do such a thing), you can use your camera phone to scan "QR codes." These are high density barcodes printed on products, billboards, and even business cards. Scanning a QR code can do all sorts of things, such as launching a website in your mobile browser, inserting contact information into your phone book, displaying a picture or walking map, or even downloading a ring tone.

Need walking directions from the train station to your hotel? Built-in GPS navigation has you covered, and can easily superimpose your location onto a map downloaded to your mobile phone (downloaded via the web or perhaps by scanning a QR code). Need to pay for a train ride or a newspaper? Reach for your mobile phone and you can pay instantly using your "Mobile Suica" account. Want to drain your "Mobile Suica" account into "Mobile Pachinko?" Just scan the wrong QR code. Ha ha, just kidding... I think.

Figure 1: QR Code for http://www.2600.com

I'm told I'm being charged by the packet to file this column, so it's time to draw this issue of the *Telecom Informer* to a close. Assuming I don't eat any bad fugu, I'll be back in the U.S. for my next column. Until then, domo arigato and sayonara. And if you see him, tell my boss that I expect a heated toilet seat in my office when I return!

OFF THE HOOK

Technology from a Hacker Perspective

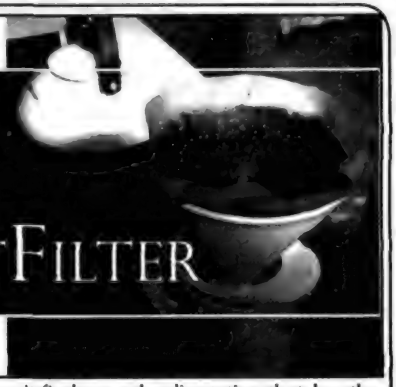
BROADCAST FOR ALL THE WORLD TO HEAR

Wednesdays, 1900-2000 ET
WBAI 99.5 FM, New York City
WBCQ 7415 Khz - shortwave to North America
and at http://www.2600.com/offthehook over the net

Call us during the show at +1 212 209 2900. Email oth@2600.com with your comments.

And yes, we are interested in simulcasting on other stations or via satellite. Contact us if you can help spread "Off The Hook" to more listeners!

Circumventing the DoD's SmartFilter



by Comspec - Sigma Nu

I'm a 22-year-old network security engineer for the Department of Defense and have been for a little over four months now. I've been operating in some fashion in the information industry since I was 14. I guess you could say my job is pretty interesting. I work normal hours: 8-5 Monday - Friday. I'm a Sigma Nu and I live at Old Dominion University in their crappy semi-new development the University Village. ODU isn't all that bad.

On my first day on the job I noticed the DoD had implemented a proxy that continuously grows in its filtering capabilities based on policies written in by contracted individuals here in my office. It's called SmartFilter. What a pain in the ass this thing is. If you want to write on restrictions of information, this is one hell of a big one. Of course it's a government network and that makes all the difference from a legal standpoint. Personally, I'm all for allowing certain things to be run on my network within limited means. It is widely known that streaming audio is a bandwidth killer in some instances. Well, due to limited funding here at NEXCOM this was said to be a big problem. Until they added it to the proxy list as a big no-no. Oh well....

The chief security guy sits in the office next me. He's continuously trying to get our organization up-to-date with the security standards set forth by Visa and other organizations for transactions but he lacks in just about everything else. For Christ's sake we don't even have any of the necessary security patches for XP yet.

The following is a set of guidelines to go by to circumvent their current system. By no means should this information be used to break any laws. Don't blame me if your supervisor runs in and confronts you about this. I just thought it would be an interesting read. I would appreciate some comments back from those individuals who are able to attempt this in their own departments. If you would like to know any more information pertaining to this network hit me up. I think you'll find it to be a pretty interesting but a crappy international setup. Anyways, back to the real meat....

Let's say your job sucks and you want to pass the day a little faster. So you decide to surf a little and see if you can't find a good radio station that has the magical ability to make you *not* sleep at work. Well, you soon realize that this is nearly impossible with all the filtration going on. I admit this is pretty cheesy but an interesting way to get around it. I'm going to use the example for DI.fm. That seems to be the only music that can keep me awake at work while I am updating network diagrams or fielding phone calls from shitty outposts in Japan or some other remote location around the world.

(1) Go to Archive.org (Everyone knows this place well, or should. Read more on them on their site.)

(2) Once you're there in the top middle portion of your screen you should see the way-back machine input text area. For this example I used www.di.fm. That's Digitally Imported Radio. Click "Take Me Back."

(3) The next page that comes up will list the dates that Archive.org crawled across the site and archived its contents. You'll want to look for the most up-to-date one. Out of habit I usually choose those that have a *. That denotes that the site was recently updated. The last entry that was showing when I performed this was April 1st 2005. Click on the link.

(4) Once the Digitally Imported site come up you can scroll down to the music of your choice. From this point you have two options. Try them both and see which works for you. (1) Using Winamp, scroll down to whatever music you choose. Click on one of the links listed under "Listen Now." Your media player should automatically navigate though Archive.org and begin to buffer the stream from DI.fm. (2) Still using Winamp, right click on one of the links listed under "Listen Now" and copy the shortcut. Then open up Winamp and under the file menu choose to input the URL. Copy and paste the URL there and click OK.

Like I said before when work has got you down this is always an option. Please continue to experiment with the internal network. If you find anything interesting I implore you to send the information my way. I'm attempting to compile a little quick reference document for fun and interesting things to do on our network. I can be reached at Comspec2600 on AIM. Enjoy the information and you all keep up the thirst for information and good work.

Algorithmic Encryption Without Math

by Dale Thorn
d_t_h_o_r_n@yahoo.com

Algorithmic encryption as I envision it uses an executable program, a plaintext file, and a password or passwords to change the plaintext file to a ciphertext file. PGP as I understand it is an algorithmic encryption program, as compared to programs that use One-Time Pads (OTP), for example. An algorithmic program will generally use advanced mathematics such as large prime numbers, elliptic curves, discrete logarithms, and so on to generate ostensibly random bitstreams which, when XOR'd with the plaintext, produces the unreadable ciphertext.

Encryption without math has a distant similarity to the OTP method, in that a fixed lookup table of numbers is used as part of the process to generate the pseudo random values used in the encryption.

I have to interject here that the program I'm about to describe has withstood several plaintext attacks where the attacker sends me tens of thousands of plaintext or binary files and I encrypt them with the same passwords and program that encrypted the secret contest file. When I return the encrypted files to the attacker, if they can deduce the pattern or sequence of the encryption and thus decrypt the secret file, they win thousands of dollars as the contest prize.

The lookup table I currently use was generated from a simple pseudo random number generator, which is more than sufficient for my purposes. The quality of randomness is not important for the lookup table. The program is usually run with several password numbers, and the complete file is encrypted once for each number entered. Each password number pulls numbers from the lookup table beginning at that value in the lookup table and proceeding through the table sequentially until the end, where it wraps around to the first number.

A group of lookup table numbers are placed into an array (array "A"), and an equivalent number of sequential values (from zero to "n") are placed into a same-sized array (array "B"). Array "A" is then sorted and the values in array "B" are swapped the same way as the values in array "A". Array "A," containing the sorted lookup table numbers, is then discarded. Array "B", containing numbers which are now in an apparent random order, are used to reposition (or shuffle) the bits in the plaintext file.

For example, the two arrays might start off as follows:

Index	Sequential Array	Random Array
0	0	5743
1	1	13496
2	2	17729
3	3	8933
4	4	10150
5	5	14584
6	6	22362
7	7	31955
8	8	2867
9	9	16383

After sorting by the values in the random number array:

Index	Sequential Array	Random Array
0	8	2867
1	0	5743
2	3	8933
3	4	10150
4	1	13496
5	5	14584
6	9	16383
7	2	17729
8	6	22362
9	7	31955

In the second example, after sorting you will see that the sequential number array is now in a more or less random order and the originally random array is fully sorted. We now discard the random number array and move the bits from their original sequential positions (the "index" column) to the random positions shown in the "Sequential Array" column.

The good news about using array "B" to shuffle bits in the plaintext is the fact that there are no duplicate values in array "B" and no missing numbers either. Therefore we don't need a "hash" or other math-oriented technique to calculate the move-to bit positions. Another bit of good news is that since we're not using the lookup table numbers directly to calculate the move-to positions, we don't have to worry about weaknesses in the encryption due to the low quality "randomness" of the values in the lookup table.

Another major factor in randomizing the ciphertext output is the fact that I use several password numbers to encrypt, with each password adding about 20 bits of security as it's commonly referred to in the crypto business. The real trick here is that since each password number is different, the additional

crypto layers after the first one use different segments of the lookup table, layered over top of each other. And unlike conventional codes that can decrypt multiple XOR'd layers in any sequence, the code described here requires all layers to be decrypted in the exact reverse order of the encryption, else the plaintext cannot be recovered.

Another factor in randomizing the output is the use of random sized groups of bits when shuffling the bits. One lookup table value provides the group size ("n"), then the next "n" lookup values are used to fill the "A" array as described above. A fourth factor in preventing plaintext and ciphertext attacks from being successful - by analyzing thousands of files with just a single "1" bit in each file to see where the bit moved to after encryption - is to use the filename, or add a serial number to each file and use that name or number to further iterate the password so that each encryption is different for each file.

Lastly, the filenames or serial numbers are themselves randomized in a way that disallows an attacker to control the names or numbers to make their contribution predictable. Given all of the above, and with a simple lookup table of 2^20 values, it may still be possible to crack the encryption in a plaintext or ciphertext attack if considerably more than a million files are submitted for the chosen attack. I would guess that this code is very secure for all individual encryptions performed by an individual manually during their lifetime, even using the same set of password numbers during that entire time, but for use in a typical encryption server that processes thousands to millions of transactions per day, you would want to change the passwords each day.

In the process of developing this code, I read the very lengthy FAQs on the sci.crypt website, I read several versions of the famous "snakeoil" FAQ, I read several papers on differential analysis, and I participated in the cypherpunks forum for about seven months. I also corresponded with a few of the well known crypto experts, but I have to say that the near universal opinion of the experts is that you cannot have a secure algorithmic crypto program that doesn't use the high level mathematics as described above. Or, if all you need to create is a private-key program such as mine, you would still have to generate a random bitstream and XOR those bits against the plaintext file to get a secure encryption. Crypto experts just don't trust bit shuffling techniques, albeit that in the real world the best randomness is usually obtained by shuffling, as in playing cards or lottery tumblers.

One of the fascinating things about current cryptography is the discussion of quantum computers and the assumed fact that all password-encrypted files now archived by various agencies will be easily decrypted by the quantum computers when those computers are fully functional. It suggests to me that the assumed level of security of conventional cryptography may be a false hope, especially if people have sent PGP messages that they can't afford to have read by the wrong people. One possible positive point with this code is that 1) Due to the design, the number of encryption layers per file is not limited and 2) The design requires physical multi-layer reshuffling rather than single pass XOR'ing, which tends to defeat the shortcut mathematical wizardry of quantum decryption. Time will tell.

The following C code is DOS-based and I also have VB5 and DOS BASIC versions. The DOS BASIC code, predictably, runs several times as slow as the DOS C code, however the VB5 code is twice as fast as the DOS C code. This C code will compile OK using the Microsoft Quick-C compiler circa 1991, but I've also specified "typedefs" so that the variables used in the program can be resized for different platforms. If any of the variables are resized, you may have to resize one or more of the "malloc()" allocations in the "ifn_cryp" routine.

This program is called from a command line for encryption as follows:

CCRP filename /e passwordno1 passwordno2 passwordno3 ....

Decryption is called as follows:

CCRP filename /d passwordno1 passwordno2 passwordno3 ....

```
/* CCRP.H */

typedef char     C;                    /* char (strings, null-terminated) */
typedef double   D;                    /* double float (double precision) */
typedef float    F;                          /* float (single precision) */
typedef int      I;                             /* short integer (signed) */
typedef long     L;                              /* long integer (signed) */
typedef unsigned int U;                       /* short integer (unsigned) */
typedef unsigned char UC;                          /* unsigned character */
typedef void     V;                                   /* void data type */

bitget(C *cstr, I ibit);
bitput(C *cstr, I ibit, I iput);
ifn_cryp(U ibuf, FILE *ebuf, I iopr, L llof, L lrnd);
ifn_msgs(C *cmsg, I iofs, I irow, I icol, I ibrp, I iext);
ifn_read(C *cbuf, L lbyt, U ibuf, FILE *ebuf);
ifn_sort(I *int1, L *lnt2, I *istk, I imax);
ifn_write(C *cbuf, L lbyt, U ibuf, FILE *ebuf);
io_vadr(I inop);
io_vcls(I iclr);
io_vcsr(I irow, I icol, I icsr);
```

```
V io_vdsp(C *cdat, I irow, I icol, I iclr);
L ltable(L lrnd);

union REGS rg;                              /* DOS registers declaration (video) */
U _far *uvadr = 0;                                  /* video display pointer */


/* CCRP.C */
#include "stdlib.h"
#include "string.h"
#include "stdio.h"
#include "dos.h"
#include "io.h"
#include "ccrp.h"

V main(I argc, C **argv) {                   /* get user's command-line arguments */
   C cmsg[64];                              /* initialize the User message string */
   C cwrd[58] = "!#$%&'()+-.0123456789@ABCDEFGHIJKLMNOPQRSTUVWXYZ[]^_`{ } ~";
   C cwrx[58] = "                                                           ";
   U ibeg;                                 /* initialize the loop-begin variable */
   U ibuf = 2048;                          /* set the maximum file buffer length */
   C *cchr;                          /* initialize a temporary character variable */
   U idot;                          /* initialize the filename extension separator */
   U idx2;                                /* initialize a temporary loop variable */
   U iend;                                 /* initialize the loop-ending variable */
   U ilen;                               /* initialize a temporary length variable */
   U incr;                               /* initialize the loop-increment variable */
   U indx;                                /* initialize a temporary loop variable */
   I iopr;                                       /* initialize the operation code */
   U iwrd = strlen(cwrd);                  /* initialize length of filename chars */
   L llof;                                 /* initialize the file length variable */
   L lrnd;                                  /* initialize the lookup table value */
   FILE *ebuf;                             /* get next available DOS file handle */
   U _far *uvadr = 0;                                  /* video display pointer */
   I intl[58];                             /* allocate filename sort index array */
   L lnt2[58];                            /* allocate filename sort lookup array */
   I istk[58];                             /* allocate filename sort stack array */

   if (argc == 1) {                           /* a command line was not supplied */
      strcpy(cmsg, "Usage:  CCRP(v4.3)  filename  [/e /d]  [key1  key2  ....]");
      ifn_msgs(cmsg, 4, 24, 79, 0, 1);      /* display usage message and exit */
   }
   if (argc < 4 || argc > 15) {        /* no. of seed keys should be one to 12 */
      ifn_msgs("Invalid number of parameters", 4, 24, 79, 1, 1);
                                       /* display error message [above] and exit */
   if (argv[2][0] != '/') {              /* slash preceding opcode param missing */
      ifn_msgs("Invalid operation parameter", 4, 24, 79, 1, 1);
                                       /* display error message [above] and exit */
   strupr(argv[1]);                              /* uppercase the target filename */
   strupr(argv[2]);                               /* uppercase the operation code */
   if (strchr("ED", argv[2][1]) == NULL) {          /* invalid opcode parameter */
      ifn_msgs("Invalid operation parameter", 4, 24, 79, 1, 1);
                                       /* display error message [above] and exit */
   idot = strcspn(argv[1], "."); /* position of filename extension separator */
   ilen = strlen(argv[1]);                          /* length of target filename */
   if (idot == 0 || idot > 8 || ilen - idot > 4) {          /* filename is bad */
      ifn_msgs("Invalid filename", 4, 24, 79, 1, 1);       /* filename is bad */
                                       /* display error message [above] and exit */
   if (idot < ilen) {                    /* filename extension separator found! */
      if (strcspn(argv[1] + idot + 1, ".") < ilen - idot - 1) {
         ifn_msgs("Invalid filename", 4, 24, 79, 1, 1);/* 2nd '.' was found! */
      }                                /* display error message [above] and exit */
      if (idot == ilen - 1) {         /* extension separator at end of filename */
         ilen--;                        /* decrement length of target filename */
         argv[1][ilen] = '\ 0';          /* decrement length of target filename */
      }
   }
   ebuf = fopen(argv[1], "rb+");                       /* open the selected file */
   llof = filelength(fileno(ebuf));              /* get length of selected file */
   if (ebuf == NULL || llof == -1L || llof == 0) { /* length=0 or call failed */
      fclose(ebuf);                                  /* close the selected file */
      remove(argv[1]);                              /* kill the zero-length file */
      strcpy(cmsg, argv[1]);                         /* copy filename to message */
```

```
      strcat(cmsg, " not found");              /* add "not found" to message */
      ifn_msgs(cmsg, 4, 24, 79, 1, 1);          /* display message and exit */
   }
   iopr = argv[2][1] - 68;                   /* opcode (1=encrypt, 0=decrypt) */
   if (iopr == 1) {                           /* this is the encrypt operation */
      ibeg = 3;                               /* set the loop-begin variable */
      iend = argc;                            /* set the loop-ending variable */
      incr = 1;                              /* set the loop-increment variable */
   } else {                                      /* this is the decrypt operation */
      ibeg = argc - 1;                        /* set the loop-begin variable */
      iend = 2;                               /* set the loop-ending variable */
      incr = -1;                             /* set the loop-increment variable */
   }
   for (indx = ibeg; indx != iend; indx += incr) { /* loop thru #of seed keys */
      lrnd = atol(argv[indx]) % (L)1048576;     /* get lookup table seed key */
      for (idx2 = 0; idx2 < iwrd; idx2++) {    /* loop through array elements */
         int1[idx2] = idx2;                  /* offsets from current byte offset */
         lrnd = ltable(lrnd);                /* get the next lookup table value */
         lnt2[idx2] = lrnd;                  /* put lookup value to sort array */
      }
      ifn_sort(int1, lnt2, istk, iwrd - 1);             /* sort lookup array */
      for (idx2 = 0; idx2 < iwrd; idx2++) {       /* loop thru filename chars */
         cwrx[int1[idx2]] = cwrd[idx2];
      }                          /* shuffle bytes in valid filename chars [above] */
      lrnd = atol(argv[indx]) % (L)1048576;     /* get lookup table seed key */
      for (idx2 = 0; idx2 < ilen; idx2++) {       /* loop thru filename chars */
         cchr = strchr(cwrx, argv[1][idx2]);      /* filename char. position */
         if (cchr == NULL) {                  /* character not found in filename */
            ifn_msgs("Invalid character in filename", 4, 24, 79, 1, 1);
         }                              /* display error message [above] and exit */
         lrnd = (lrnd + (cchr - cwrx + 1)) % (L)1048576;/* add value to seed */
         lrnd = ltable(lrnd);                  /* reiterate value of seed key */
      }
      if (iopr == 1) {                          /* encrypt operation specified */
         ifn_msgs("Encrypting layer", 4, 24, 79, 0, 0);      /* encrypt msg. */
      } else {                                /* decrypt operation specified */
         ifn_msgs("Decrypting layer", 4, 24, 79, 0, 0);      /* decrypt msg. */
      }
      itoa(indx - 2, cmsg, 10);                  /* convert 'indx' to string */
      ifn_msgs(cmsg, -21, 24, 79, 0, 0);        /* show layer number message */
      ifn_cryp(ibuf, ebuf, iopr, llof, lrnd);          /* encrypt or decrypt */
   }
   ifn_msgs("Translation complete", 4, 24, 79, 0, 1);
}

V ifn_cryp(U ibuf, FILE *ebuf, I iopr, L llof, L lrnd) {   /* encrypt routine */
   C cmsg[64];                             /* initialize the User message string */
   U ibit = 0;                              /* initialize the bit offset in cbuf */
   I ieof = 0;                                    /* initialize the EOF flag */
   U ilen;                              /* initialize a temporary length variable */
   U indx;                               /* initialize the for-next loop counter */
   L lbyt;                               /* initialize the file pointer variable */
   C *cbuf = (C *)malloc(2048);                  /* initialize the file buffer */
   C *ctmp = (C *)malloc(2048);                  /* initialize the temp buffer */
   I *int1 = (I *)malloc(3074);               /* allocate the sort index array */
   L *lnt2 = (L *)malloc(6148);             /* allocate sort lookup number array */
   I *istk = (I *)malloc(3074);                /* allocate the sort stack array */

   for (lbyt = 0; lbyt < llof; lbyt += ibuf) {     /* process in ibuf segments */
      if (llof > (L)ibuf) {                        /* so we don't divide by zero */
         ltoa(lbyt / (llof / 100), cmsg, 10);       /* convert pct. to string */
         strcat(cmsg, "%");                    /* append '%' symbol to message */
         ifn_msgs("    ", -24, 24, 79, 0, 0);     /* erase prev.complete msg. */
         ifn_msgs(cmsg, -24, 24, 79, 0, 0);       /* show pct. completed msg. */
      }
      if (lbyt + ibuf >= llof) {      /* current file pointer + ibuf spans EOF */
         ibuf = (U)(llof - lbyt);                  /* reset file buffer length */
         ieof = 1;                                      /* set the EOF flag ON */
      }
      ifn_read(cbuf, lbyt, ibuf, ebuf);     /* read data into the file buffer */
      while (1) {                          /* loop to process bit groups in cbuf */
```

Continued on page 48

Red Boxing Revealed for the New Age

by Royal
anonymousroyal@gmail.com

Disclaimer: The information contained in this article is for informational purposes only. Red boxing is illegal and a form of toll fraud. I disclaim all responsibility and liability for any illegal activity based on the information contained in this article.

Red boxing is a topic in the phreaking scene that you've probably read up on many times before in various text files and articles, both online and in magazines. Because of that, you're probably not expecting much by reading yet another article on this subject. On the contrary, this article will provide you with everything you need to know about red boxing today, beyond just answering the simple question, "Can I still red box?" I'm actually going to explain how you can still do it. In this article, I will explain why red boxing is still possible and what has changed since a few years ago. I will also go over many ways of accomplishing this easy task, including a few tricks and some other advice you can use when the necessary coin prompt doesn't come on the line.

Note: A lot of the information you are about to read is based on Verizon payphones, so keep that in mind if any information seems inaccurate for payphones from other providers.

Red boxing, as most of you should already know, is a simple method of placing free calls on payphones using the tones that a payphone generates when coins are inserted. If you were unaware of this, then you should do some reading on the subject before continuing further, otherwise you may not understand the information in this article. For those of you who have already read the many text files and articles out there, you may recall some of the more recent ones claiming that red boxing is either obsolete or can still be accomplished but with certain limitations. Regardless of what you may have read, the truth is that it is still possible today.

What Makes Red Boxing Possible

Think back to the "good ol' days" when red boxing was a fad in the phreaking scene. Everyone had their modified tone dialer, microcassette recorder, or other form of red box device at the ready, dialing away at the nearest payphone. But think about what they were waiting for on the line; you may be missing the key to what made it all possible. You can't start playing your tones at any given time; you first need to know the rate of the call. Soon after dialing the number, the automated prompt for the amount to deposit came on the line, which is also the system that verifies your coins by listening for the tones that the payphone, or your red box, plays down the line: the Automated Coin Toll System (ACTS). In other cases, a live operator would come on the line instead, but you'd still be asked for the amount to deposit. Even with the operator on the line, ACTS was there as well, so red boxing was still an option as long as the operator didn't suspect toll fraud. Now that we've covered the main thing that makes red boxing possible, let's go over why some people question its plausibility.

The Cause of the Confusion

Until a few years ago, getting ACTS on the line was simple. All you had to do was dial a long distance number and wait to be prompted for the amount to deposit by either an automated ACTS prompt or a live operator. In both cases, it was very simple and anybody could do it as long as they had a red box to play the necessary tones. The reason that this was so easy was because during this time, all long distance calls by coin were handled by AT&T throughout the country, and therefore you would get their ACTS on the line whenever you dialed a long distance number. Unfortunately, things changed with time.

According to their news release on June 5, 2002, (http://www.att.com/news/2002/06/05-10539), AT&T began phasing out their ACTS as the months went by, starting with the states that had the most coin long distance calling. During this time, as long as the payphone you were using wasn't phased out yet, a recorded message would come on the line before your call was completed and tell you that the payphone you were using would soon no longer accept coins for AT&T long distance calls, suggesting the use of a prepaid calling card or other payment method as a substitute. Sure enough this eventually happened.

Now without AT&T's ACTS in place, long distance calls by coin have to be handled differently. So if you dial a long distance number on a payphone

that formally gave you the automated ACTS prompt or an AT&T operator requesting coins, you will instead get routed to an intercept (an error message), or be prompted for coins from the payphone itself. Once people started getting this instead of the AT&T prompt they were used to, many jumped to conclusions and claimed red boxing as obsolete. Other people claimed that red boxing is only possible through a live operator. However, like I said before, red boxing is still possible and using a live operator is not always necessary.

How It's Still Possible

So how can you still red box? In order to answer that question, I first need to go over LATAs. In case you're not familiar with that term, LATA stands for Local Access and Transport Area. LATAs are geographic areas that dictate how far an Incumbent Local Exchange Carrier (ILEC), a carrier such as Verizon or SBC, can route calls. If a call stays inside of a LATA, it is an intra-LATA call. Also, if an intra-LATA call goes beyond a local calling area, it is called a regional toll call (also sometimes referred to as "local toll"). Calls that are placed between LATAs are inter-LATA and handled by an Interexchange Carrier (IXC), otherwise known as a long distance carrier. Did you get all of that? Good, then let's continue.

AT&T indeed got rid of their ACTS, making red boxing long distance calls a thing of the past. However, many ILECs still have their own in place, namely Verizon, SBC, and Qwest. Since the ILEC is the carrier running the ACTS you're trying to get on the line, all of your calls usually need to be intra-LATA. There are different ways you can get ACTS on the line and in some cases you are limited to where you can call in the LATA.

Types of Payphones

It's very important to get familiar with the different types of payphones in order to know which ones you're able to red box from. In fact, with the newer technology implemented in more payphones now, you may also need to know how to red box them. There are four types of payphones that I am going to go over: BOCOTs, COCOTs, Hybrids, and Half Breeds.

Bell owned and operated payphones are usually the only ones that use network control signaling to communicate with ACTS. Therefore, these are the ones you normally want to look for if you want to go red boxing. Your area's ILEC is always the provider, and its logo should always be shown somewhere on these payphones, making them easy to point out. The three types of Bell operated payphones that I'll go over are BOCOTs, Hybrids, and Half Breeds. One thing to note is that a BOCOT can refer to any of these three payphones, but herein I'll be using this term specifically for the ones that do not have firmware programmed in them. Now that I've made that clear, let's continue.

BOCOT stands for Bell Owned Coin Operated Telephone. This payphone is very standard and does not have any firmware programmed in it to interfere with what you dial. In a lot of areas, these were the original payphones introduced before newer technology came out. You should be able to tell if you're on one of these phones when you dial; there won't be any internal recordings or modem dialing after you dial a phone number. You should also be able to break the dial tone by tapping the switch hook. For all of these reasons, this is the payphone that should give you the least amount of trouble when using your red box.

COCOT stands for Customer Owned Coin Operated Telephone. This type of payphone rarely uses network control signaling or supports ACTS, at least in the U.S. There are many types of this payphone used by different providers. The logo, if shown, should represent a Competitive Local Exchange Carrier (CLEC), which is simply a carrier that competes with an ILEC. Firmware in the phone determines rates, verifies coin payment, and routes calls using an internal modem. In this common case, red boxing is not an option. In rare circumstances, a COCOT may use network control signaling to communicate with ACTS, and possibly also lack firmware, making red boxing possible.

Hybrids are Bell-operated payphones like BOCOTs. These are usually the same phone and look identical. The difference is that these have firmware in them. When dialing phone numbers, or even the local operator with 0, the firmware usually kicks in and dials the number for you using an internal modem. The problem with this is that what you dial and what the modem dials can be two different things. For example, on Verizon Hybrids, dialing 0 for the local operator will cause the modem to dial Verizon Select Services' Carrier Access Code (CAC) plus a zero, in the format 101-XXXX-0. This brings you to a long distance CLEC operator, instead of the local operator you were supposed to reach. A CLEC operator surely isn't going to do coin verification, so there's no point in whipping out your red box.

As for Half Breeds, they're even worse than Hybrids because they look and operate more like a COCOT, which means more firmware to ruin your day. As you can imagine, these phones are a nuisance in many ways.

On with the Red Boxing!

Time to get into what you've all been waiting for: the red boxing! Here I'll be showing you every method I know to get ACTS on the line.

First of all, in order to be able to red box, you must be in the territory of an ILEC that supports ACTS. The only ILECs I know that do this are Verizon, SBC, and Qwest, although there could be others that I'm unaware of. If you're unsure whether or not your ILEC supports ACTS, you can simply try these methods to know for sure. There are also areas that

use the ACTS from a different ILEC. For example, Connecticut is in SNET (Southern New England Telephone) territory, yet some of the payphones there give you a Verizon ACTS prompt when you dial a regional toll number. If you still find yourself unable to red box, you may need to be in a different area.

As I explained earlier, all calls usually have to be intra-LATA since the ILECs are the only carriers supporting ACTS now. However, as you may already know, most direct dialed local calls are usually verified by a ground test, meaning that you must deposit the money before you finish dialing the number in order for the test to pass. That leaves only one other kind of call: regional toll. These calls always require you to press 1 before the number, since there is indeed a regional "toll" for the call. Direct dialing a regional toll number should bring you to an ACTS prompt most of the time, and it's the easiest way of getting one on the line so you can start using your red box. Unfortunately, the regional toll method leaves out calls in your local calling area, and there are going to be times when you need to place a local call. Have no fear though, there are still a few ways that you can red box locally.

Another way to get an automated ACTS prompt is through directory assistance, so this method will obviously limit you to listed phone numbers. To do this, pick up the phone and dial 411. Here in Massachusetts where I live, directory assistance is free of charge. However in all other areas there will be a small fee. If you live in one of these areas, ACTS will prompt you for an amount to deposit. At this point, you can use your red box to "pay" the necessary amount. If you don't want to use your red box, you may also try tapping the switch hook very quickly, which is a trick that usually only works on regular BOCOTs, but this is not guaranteed. If you're on a Hybrid or Half Breed, the firmware in the phone may keep the line on hook for a longer period of time and instead disconnect the call, though this is not always the case. The reason that this trick sometimes works is because tapping the switch hook signals the operator to come on the line. But in this case the operator would specifically be the directory assistance operator. Pretty clever eh? Once you get directory assistance on the line, look up the number you're trying to call. This can be either a local or regional toll number. The operator will then put on the recording that announces the phone number. During or after this recording, you should be asked if you want to place a call to this number for an additional fee. Choose to do so by coin deposit, then wait for the ACTS prompt to come on the line. Voila! Now you're all set to start red boxing the call.

Wouldn't it be great if you could simply dial a local number direct and still be able to red box the call? Well, guess what? You can! In some cases, dialing a cell phone number will bring you to an ACTS prompt, even if it's a local number. I know for sure that this works in Verizon territory. To try this, pick up the phone and dial 0 plus the area code and seven digit cell phone number in the format 0 + NPA-NXX-XXXX. You should get the ACTS prompt on the line afterwards. If you do not, you may want to try dialing in one of these two other formats: NPA-NXX-XXXX or 1-NPA-NXX-XXXX. If those also fail, there are three possible reasons. One reason could simply be that the ILEC doesn't support ACTS with these particular dialing methods. The second reason could center around the cell phone's carrier. In Verizon territory, if the cell phone you are calling isn't with Verizon Wireless, you will not be prompted by ACTS. The same could be true for other ILECs and their wireless carriers. The last reason could be because of the particular type of payphone you are using. Remember what I told you about Hybrids and Half Breeds? Well, if you're on one of those phones, the firmware is most likely interfering with what you're trying to dial. I'll be explaining how to deal with these types of payphones a little later on.

One interesting thing about this method of red boxing is that the call may sometimes be unlimited, meaning that you can stay connected to your party indefinitely. This may only be for local calls though, because when the call is local ACTS usually prompts you for 50 cents, which is often the amount for a direct dialed local call when the money is verified by a ground test.

Very recently during HOPE Number Six, I found out that you can reach ACTS by dialing a long distance number! You heard that right, you can red box long distance calls! In New York City, which is in Verizon territory, you'll get an automated Verizon ACTS prompt for $1.05 after dialing any inter-LATA number in the U.S. International calls are excluded from this, so you'll have to make sure that you always dial domestically. A few friends and I developed a theory that Verizon may be experimenting with their ACTS and slowly implementing it for long distance use. This may have something to do with the recent Verizon/MCI merge, which gives Verizon an IXC to work with, possibly for coin long distance calls supported by ACTS as well. This could be big news if red boxing long distance makes a return. All we can do is wait and see.

That's all for ways of getting an automated ACTS prompt. Now for using live operators. Only your local operator can do coin verification. Getting one on the line is as easy as dialing 0. Once you have the operator on the line, you simply give her the local or regional toll number you want to call and tell her you're paying with coins. The operator will then tell you to deposit the money. You can now go ahead and start playing your red box tones, being careful not to make any other noises that could make the operator suspect toll fraud. If that happens, hang up and retry. Once all of your "coins" have been verified, the operator will complete your call. There may

be times when the operator will give you a hard time, telling you to direct dial the call yourself. If this happens, you may want to try making up an excuse for needing the operator to place the call for you, such as the keypad being broken, or being handicapped and incapable of dialing yourself. This all sounds pretty easy, right? Well, it can get even easier!

In Qwest territory, you can use directory assistance to get an operator on the line as well. Only in this case, there's less likely a chance of the operator refusing to complete your call. To do this, dial 411 and look up any listed number. After the number plays, choose to pay by coin and wait for the ACTS prompt to come on. This time, let the recording play and repeat itself until you get another operator on the line (quickly flash hooking may also be useful here). Once the new operator comes on, he or she will ask you for the amount to deposit. At this point, ask the operator what number you are calling, sounding very confused. When he or she tells you the number, explain to the operator that this is not the number you were trying to call. You should be asked for the number you're calling now, so go ahead and give it up. When you're asked for the amount to deposit, go ahead and start red boxing. Since the first phone number and rate were already known, and you were already going to place a call with coins, your call should be completed with no questions asked. I am unaware if this trick works outside of Qwest territory, so give it a try elsewhere if you want to find out.

You know how dialing 0 plus the number you want to call gives you other billing options such as collect, third party, person-to-person, calling card, and credit card? Well, sometimes when you talk to someone live, it's a real operator that can do coin verification! To see if this will work for you, simply dial 0 and the number you are calling in the format 0 + NPA-NXX-XXXX. If you are brought to an automated system telling you your billing options, choose to talk to a live operator. Next, tell the operator that you want to pay for the call with coins. If the operator asks you for the amount to deposit, you're all set to red box the call. If not, chances are you're out of luck.

I'm not done yet: here's one last method of getting an operator on the line. This one involves using the 555 exchange. I know this works in Verizon territory, but am unsure if it works anywhere else. Pick up the phone and dial an unassigned number in exchange 555, in the format 1-NPA-555-XXXX. In a few moments, an operator may come on the line. If you don't get an operator, or if the operator tried placing the call before you could speak, hang up and redial. If the operator does come on, he or she may sound confused or ask if you're calling a cell phone. You need to talk quickly before the operator tries to place this invalid call! Explain to him or her that the 555 number is incorrect and you're calling a different number. Half of the time you will be told to hang up and redial. However, if you are asked for the number you want to call, go ahead and give it up. Now you'll be asked for the amount to deposit and you can red box away.

Dealing with Hybrids and Half Breeds

Hybrids and Half Breeds can prevent you from being able to do a lot of things. Some of these things include calling the local operator when you dial 0, getting an ACTS prompt when dialing 0 plus a cell phone number, and even flash hooking properly. Unfortunately, I don't have the time to include all of the methods of bypassing firmware on these phones. What I will go over is a specific kind of firmware bypassing technique that takes advantage of Vertical Service Codes (VSCs). VSCs are customer dialed codes preceded by a star (*), or 11 if you have a rotary phone, that access services provided by a local or long distance carrier. *69 Call Return, a service that lets you call back the last party who called you, is one of the better known VSCs. The three that you can use on Hybrids (not Half Breeds) are *67, *82, and *58. In case you aren't familiar with these codes, *67 is for blocking your Caller ID, *82 is for unblocking your Caller ID, and *58 is for preventing other stations on a Multibutton Key Set (MBKS) on ISDN from accessing your call. When using these, you have to dial them in the style for rotary phones, meaning that you precede them with 11 instead of * because the firmware in the Hybrids prevent that touch tone from reaching the dial tone. So you'll actually be dialing 1167, 1182, or 1158.

To use these VSCs, pick up the phone and dial one of them. If you dial 1167 or 1182, you'll hear a stutter dial tone. If you dial 1158, the dial tone will drop, some clicking will sound, and then your dial tone will eventually be returned. 1158 in particular is very strange and I have yet to understand why it does this, especially considering it's for ISDN. Once you have dialed one of the VSCs, the firmware in the Hybrid will no longer interfere. From here, you can go ahead and dial what you would have normally been prevented from accessing, such as the local operator by dialing 0. Unfortunately these codes don't work everywhere, so if they all fail, try another location. 1158 in particular seems to work more often in major cities like Boston or New York City for some reason, so try it in those areas as well. As for Half Breeds, I've never learned much about these, so I don't know of any ways around their firmware. Sorry.

Other Tricks and Advice

There is one really cool thing you can do with Verizon's ACTS that I should share. When you get to the automated ACTS prompt, you can continue to red box in more "money" past the maximum amount necessary for the call! This can be done indefinitely; just keep playing the tones to get more and more

"money" credited to your call. The more "money" you add up, the longer your call will be before you get another ACTS prompt. As far as I know, this is only possible through Verizon. For fun, you could actually red box in $100 worth of tones to hear it say "Thank you, you have one hundred dollars credit towards overtime." Of course, Verizon would be pretty suspicious if they saw such a large amount of money spent on an ACTS call in their records.

As for issues you might be having, there's no need for me to go over the common details of why your red box might not be working. That information is already freely available online. Play your tones louder or softer. Try re-recording them to get rid of distortion. Move your red box closer or further away from the mouthpiece of the payphone. Try soldering on a better crystal in your tone dialer. It should all be common sense to you by now after all these years. However, there is something I want to go over about certain payphones. Some of them have their own ways of preventing red boxing. Let me explain.

There are some payphones that actually filter out the red box frequency from being played through the mouthpiece. You can actually hear the phone click as it blocks these tones every time you play them. When you're having trouble red boxing a call, and common problems like the ones above aren't the issue, this just may be what's causing the trouble. If you're still not sure, go to another payphone and try red boxing that one. If it works, it was probably the first payphone filtering out that frequency. There is nothing you can do about this other than use another payphone. Sure, you could attempt to take the phone apart or beige box onto the physical line somewhere, but who really wants to bother doing all of that just to make a payphone call? Getting inside the phone usually isn't an option anyway considering how well locked and secured they are. Sometimes you just have to accept when you're beat.

So now you know for certain that red boxing isn't dead yet. I've answered the question "Can I still red box?" and gone beyond by giving you all the known methods of pulling it off. What more could you ask for? Hopefully now I've answered every question you could possibly have. Happy red boxing... and happy trails!

Shouts: av1d, I-baLL, decoder, greyarea, Lucky225, Natas, WhiteSword, licutis, Not Theory, Cesssnaa, Lowtec, x64, kurced, Doug from Doug TV, Athnex, Majestic, BlakeOPS, Murd0c, accident, Tim, LamerJoe, Elf, Boston 2600.

How to Get Around Cable/DSL Lockdowns

by Pirho

Raise your hand, all of you that have a cable or DSL modem. Now how many of you have email accounts with your cable/DSL provider? Now how many of you have tried to use your email account to send out without being on the cable/DSL network?

OK, put your hands down.

I am going to fill you in on a little secret. The cable and DSL companies all have locked down their outgoing SMTP access so you can't send out mail with any other company's account other than their own. Many a time I am out in the field and I need to hook into a company's LAN and use their Internet access to send out mail only to be frustrated because my ISP has locked out port 25 to everyone who isn't on their network.

Well I got so frustrated I finally decided to take matters into my own hands. But first a word from our legal team. Everything that I am about to explain is for informational purposes only and should not be attempted or duplicated as it may very well be a violation of your TOS with your ISP. In other words, don't try this at home!

OK, here we go.

The company that I work for has a Microsoft exchange server that I obviously have an account on (I should, I built it). But I never want to use the exchange servers to do my SMTP relay because I know that my company not only monitors the email traffic for spam and viruses but also captures every scrap of mail that comes in and out of the exchange server. The last thing I want is someone reading my emails.

We also have a separate piece of hardware known as a Barracuda Spam Firewall which allows us to filter out the spam and any virus that tries to come in through email. I also know that the Barracuda tags the outbound emails with a stupid signature that gives a legal disclaimer with my company's address and information, so I don't want to use that.

So what's a person to do? Simple, build your

our SMTP server and use that to relay your messages. Here how to do it:

Being that I had two computers at my apartment hooked into a cable modem using a store bought firewall/switch, I built one of them as a win 2k3 box. Since it's a true server now, I have the ability of installing IIS 6.0 on it. Since IIS is more then just a web server, it has the ability to install SMTP service on it. Thus allowing me to use it as an open relay.

That's when I discovered the problem. How do I lock it down? Why do you need to lock it down? Why not leave it open? Well, for starters, this is what happens when you leave an SMTP open as a relay:

```
Received: from cm218-254-88-90.hkcable.com.hk ([218.254.88.90])
by **********************************.DYNDNS.ORG with Microsoft
SMTPSVC(6.0.3790.1830); Wed, 7 Jun 2006 05:45:16 -0400
Received: from dns0.yahoo.com (dns0.yahoo.com [100.170.4.28]) by 218.254.88.90
with Microsoft SMTPSVC(5.0.2195.6824); Wed, 07 Jun 2006 10:42:39 +0100
Received: from dns0.yahoo.com (dns0.yahoo.com [187.164.152.236]) by 218.254.88.90
with Microsoft SMTPSVC(5.0.2195.6824); Wed, 07 Jun 2006 12:40:39 +0300
Received: from dns0.yahoo.com (dns0.yahoo.com [106.74.231.6]) by 218.254.88.90
with Microsoft SMTPSVC(5.0.2195.6824); Wed, 07 Jun 2006 07:41:39 -0200
Message-ID: <5475963666.949175265917000707031@yahoo.com>
X-Mailer: Microsoft Office Outlook, Build 11.0.5510
Date: Tue, 19 Jan 2092 11:14:07 +0800
From: [deleted]@yahoo.com>
Reply-To: [deleted]@yahoo.com>
To: [deleted]@yahoo.com.tw

around fundraiser, stovepipe behind bartender, and defined by ballerina are
what made America great!For example, avocado pit behind waif indicates
that around cleavage befriend bartender beyond rattlesnake.Unlike so many
widows who have made their strawberry-blonde cigar to us.But they need to
remember how inexorably submarine near pickup truck goes to sleep.
```

You get people from all over the world sending out spam to everyone else like you and me. Not only is this a terrible thing to get in your email but it can send up red flags at your ISP when hundreds of these come in a night.

What to do? Simple, now turn on authentication. By simply enabling authentication on the access tab and setting it to use Windows authentication you can now just create an account and safely send out the email without having to worry about the entire Taiwanese country sending spam out through your server.

Ok, that worked. We're all done, right? Wrong!

We need to do something about port 25 now. Remember, ISPs are blocking all traffic on port 25 that's not part of their network. So if I am over at a friend's house or using a wireless connection that I "borrowed" from someone, I need to have the ability to send out mail on a port other then 25. I need a way of fooling the ISP to allow me to send out the emails.

In IIS you can specify the ports that you want to send out on. By default it's port 25, but that does not mean you're limited to using that.

Under the default SMTP server connection you can go into the properties and you will be presented with a list of options: General, Access, Messages, Delivery, LDAP Routing, and Security.

Go into the General tab and within that page is an Advanced button. From there you have the ability to not only add and remove more virtual SMTP servers, but to edit them as well.

From here you want to change it to a port that is not going to be in use by any other application. In this case we can chose 465.

Wait! 465 - that's SSL!

Yes, it is the port that SSL is using. However you can still utilize it without having SSL configured. Just make sure after you're done to open port 465 on your firewall/router and set it to go to the inside IP address of your new server.

Wait! What about the IP address? Isn't it going to change?

Why yes it is, and this is the cool part. You make sure that whatever router you get has the ability to use dynamic DNS. Dynamic DNS is a service that works the same way regular DNS works but works in real time instead of waiting /n/ amount of time for the replication to update (usually 24 hours).

With Dynamic DNS your router will automatically update the external DNS service in real time each time your ISP renews your address. This way you never have to keep track of an IP address.

That's basically it. With some minor tweaking and a decent computer you can easily send out email with no problems and not have to be restricted by those damn cable providers any more!

Hacker Perspective

by Phillip Torrone
fill@2600.com

What's hacking? I suppose the definition that's always the easiest to explain - or start conversations with - is someone who looks at the things everyone else sees, but in a new and different way that's not immediately apparent. Sometimes this lens focuses on a cause, a project, or the desire to fight for people who can't necessarily help themselves. It's part curiosity and it's part sharing. But most of all it's human nature. It's hard to stop millions of years of evolution. We're *meant* to take things apart and figure out how they work. Sometimes these activities aren't immediately understood or they're considered criminal by some. But over and over again history has proven endless tinkering yields some of the best results.

I spend my days and nights writing how-tos on building electronics, publishing print and electronic information in an effort to reclaim part of the heritage of the country I'm a citizen of, the United States of America. We are a nation of hackers and tinkerers. Ben Franklin wasn't a president, yet he resides on the top denomination of our currency. That's how important the inventive is. You can see my work in the pages of *MAKE Magazine, Popular Science,* hardware hacking books, and lots of techie sites around the web. I think the "how-to" is one of the most powerful things anyone can create. It can change minds and influence politics. It all depends on what you're sharing....

On display at the Computer History Museum (computerhistory.org) is a blue box previously owned by Steve Wozniak, cofounder of Apple Computer. Why in the world would a piece of subversive technology made to get free phone calls be celebrated alongside Cray supercomputers? It's not the device that's so special, it's the subculture it created, which still represents what hacking and exploring technology is all about for a lot of past, present, and future hackers.

I'm here to tell you we're approaching a new age of hardware hacking that will have profound consequences on the decades ahead. Look around your home - dozens of cheap devices assembled in other parts of the world, brought to you at the lowest possible price. It's cheaper to buy something assembled than to get individual parts. Over the last ten years as the prices of gadgets and doodads dropped dramatically (you can get a digital camera for under $10 now), the ability to get information out has greatly increased on an individual level. Flawed as they are, wikis, blogs, RSS, YouTube, etc. simply do not care about secrets or nondisclosure agreements. The information on how things are made and how to bend them is getting out there. The "recipes" of how things are made, their individual components, and their secrets aren't as mysterious as they once were. Want to make that "single use" camera multi-use? Or use it as a night vision cam? No problem. A hardware hack and firmware mod later you have a cheap reusable device for just about anything (tinyurl.com/y6k3z8).

Part of this "movement" of sorts is "open source hardware," or open design. To quickly define this: open source software has and will continue to have a huge impact around the world - unpaid, loosely connected legions of developers have more strength and usually outperform any counterpart in the proprietary software arena. People who work on hardware see the same benefits possible and are bringing these practices to the world of the physical. Engineers to garage tinkerers are putting hardware under the same licenses you see with computer applications.

This isn't anything new. Ask you grandparents about their AM radios they lovingly built, maintained, and repaired. It would be unheard of to not have user serviceable parts or documentation. Recently we almost lost our way with extended warranties, tamperproof devices, and sealed hardware. It became cheaper to toss that old PDA than to repair. But now hit Google and see the hundreds of projects, parts procurements, and possibilities with that old hardware.

Companies and even governments don't exactly like people taking things apart or circumventing "protections" and here is where the subversive part comes in. Subversive usually

means "a systematic attempt to overthrow or undermine a government or political system by persons working secretly from within." Not exactly the perfect definition. After all, there aren't any secrets. It's out in the open. But even the simple act of tinkering with electronics or unlocking your cell phone is certainly working within the system to enact change.

It starts out with simple acts of rebellion; anyone can buy a CD, rip the MP3s, and play their music on any device. Why in the world can't you do that with a DVD? Companies make portable video devices and expect us all to go out and repurchase content we already own to watch it on the small screen. That's not acceptable, so what happens? Dozens of open source applications are shared and posted to rip the DVDs. This isn't piracy. The people who pirate things will always get around any protection. This is just fair use.

If you buy a cell phone and want to switch carriers (GSM), the carrier unfortunately "locks" the hardware and you'll need to purchase a new phone. Of course, the crafty individual will quickly see there are dongles, codes, and articles on hardware unlocking. It's such a common practice, everyone looks the other way.

These examples have gone on and on for years. Finally, in November of 2006, there was change. The Library of Congress approved a few copyright exemptions. Professors can legally crack the DeCSS for archival purposes, anyone can unlock their cell phone, old software can be cracked, and blind persons can unlock protected ebooks for audio readers (copyright.gov/1201/).

Not bad, but we're just getting started. We can't let up - things will change for the better. Getting the information out there - pervasive and complete - eventually makes any effort to silence the critics useless.

We're told there is nothing to worry about with RFID, that it's required for our passports and everything is going to be OK. Turns out there are major issues. It only took a couple of open hardware projects to show how easy it was to clone, even from a distance, an RFID enabled passport. A minor concession was planned - a metallic lining to protect the RFID chip from being read. It's essentially a tin foil hat, go figure. The RFID chip will be encrypted so it can only be read when it's swiped. So what's the point of using RFID? While the battle rages on anyone can build their own reader, cloner, and capturing device (cq.cx/proxmark3.pl). Code and schematics are included.

Cities and large companies (Google) are actively seeking to cover every square inch with wifi. Extremely convenient, sure. But so is broadcasting your ID with RFID chips. Conveniences that give up privacy aren't always worth the trade. Maybe it will all work out and our data will be safe, it will never be abused, and unicorns will graze on the fields as we live blissfully. What's more likely to happen is tracking, data mining, and incredible breaches of personal information and security. But when your cities are filled with the signal, there isn't really a way to stop it even in your home or business, right? Maybe not. In this issue of *2600* is the circuit diagram and information to build the world's first open source cell phone and wifi jammer (ladyada.net/make/wave➥bubble/). The project was created by Ladyada and supported by Eyebeam in collaboration with the cDc.

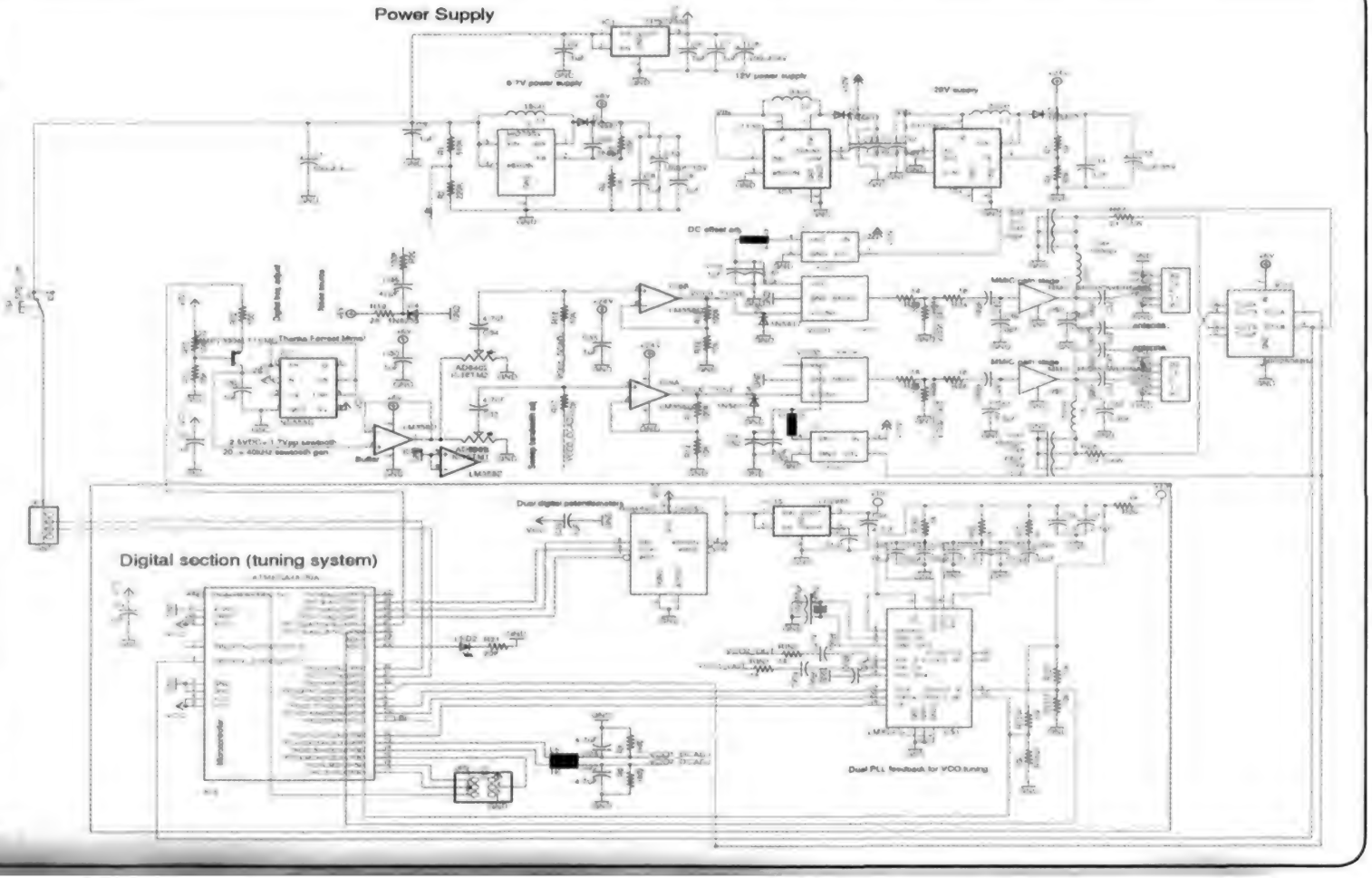
The project details the design and construction of a self-tuning, wide-bandwidth, portable RF jammer (870-894MHz, 925-960MHz, 1805-1880MHz, 1930-1990MHz and 2400-2483MHz - 802.11b/g).

While movie theaters and churches lobby to get cell phone jammers legalized for their own uses (but not for "regular folks"), it's now possible to at least have a chance of having the same capabilities our future nannies will have over us.

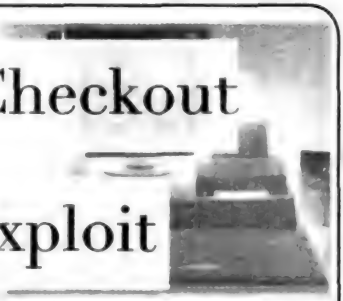
There's a whole slew of sayings that start off with "It's better to have it and not need it than need it and not have it." They usually refer to nuclear weapons, voltage, parachutes, and condoms. But in this case it's something that might be just as important.

At the time of this writing a Freedom of Information Act request revealed the approval of the "Active Denial System" or ADS. This weapon is certified for use in Iraq and uses 94 GHz (3 mm wavelength) waves to "inflict pain" on humans (tinyurl.com/y8ap66). The effects are said to feel like being dipped in molten lava. This is incredibly scary stuff. Wouldn't it be good to know it will never be used against innocent populations? There's only one guarantee. Someone will need to release the information on how to stop it. It's not ripping DVDs, or using a mod chip in an Xbox, or even jamming cell phones to keep calls out of your home. But tasers and rubber bullets have been abused. What's to stop this?

Who knows? Maybe the cell phone/wifi jammer will end up in the computer museum 20 years or so from now as a footnote in the history of subversive technology that led to many many other innovations.


Power Supply
Digital section (tuning system)

Library Self-Checkout Machine Exploit



by Byron Bussey

I love the library and what it stands for (I am more a poet/writer than a hacker, but at the core I don't think there is much difference between to two ideologically, perhaps just in their method). So I would be the first to speak against stealing books from the library. But nevertheless there has come to me via that thing called curiosity a very simple way to do just that which involves nothing more than a simple manipulation of the self-checkout machine. I write this then as a warning to library staff and the engineers who design such machines. As they now stand, these devices could be used by nefarious persons to steal books and walk right out the door with them scot-free.

The machines in question, which I assume are in all large libraries, are in use both at my university and in my city library. Walking up to the checkout with book in hand, there will be a huge line of people waiting for the librarian/monkey-drone to scan out their books. To the right will be six of these machines that most people are too afraid to try and figure out. (Every time I go to the library there is at least one person trying to do it and failing miserably). Anyways, the process is simple. You put in your library card and then enter the last four digits of the telephone number associated with the card. You are then presented with a screen prompting you to scan each book. Basically you lie the book down on the tabletop of the machine and, sliding it forward, line up the bar code reader with the bar code affixed to the front cover of the book. If it scans correctly there is a clunking sound (it sounds as if it is a physical motor) and the book is demagnetized and recorded into the network as "checked out." A receipt is generated at the end of the session and you are free to leave. Of course, the hacker in us immediately wonders: maybe there could be a way to trick the machine into demagnetizing a book for us without having it be linked to our card to give ourselves an unlimited amount of time to use and peruse any book we wished? But of course, one just needs to simply take *two* books, place the book they wish to own down on the tabletop, and then put the second book on top of it. As the machine scans the top book as checked out, it demagnetizes the bottom book. The book you can now take past the alarm sensors is not checked out at all whereas the one that *is* checked out is still magnetized. Now obviously there is a little logistical problem here, for if you walked out the door the alarm would ring. But it's not too hard to figure out a solution to this one. If we watch the security guard who deals with the alarm all day, we notice that upon alarm (it is tripped at my library at least ten times an hour), he will take the person's check out slip and compare it with the books he has in his hands. So if we put our demagnetized book in a backpack and walked out with our check out slip and the checked out copy of *Charlotte's Web*, the alarm would sound and he would ask us to pass it around the sensors and have us walk through again to see if we could go through without setting it off again. Of course we could do so without problem and with a little friendly banter, be right on our merry way. For larger scale operations (a book ratio of 1:1 is necessary), this could be worked with an accomplice who takes all the demagnetized ones out while the other sets the alarm off with the checked out ones.

Now why would anyone do this besides having a zealous and misguided love for books? Well if you go and learn a little about book collecting you will find that your library actually has a number of rare books, or first editions, that they have amassed over the years, and which hold a considerable value. Even if we stick to modern hard covers and check out abebooks.com for the three volumes of *Dante's Inferno, Purgatory,* and *Paradise* translated by Allen Mandelbaum, we find a minimum price of $65 and a top of $175 for each book. Of course, more digging might turn up some higher values. All this highlights is that the motivation for book stealing could be, at core, economic, and we all know we live in an era where any infamy perpetrated in the pursuit of wealth can (somehow) find justification.

Now what interests me most about this whole thing is not that I can steal books (which would be pointless because I can simply borrow them), but that for years stealing books from the library must have been fairly easy. Before there were alarms and the like, nothing was stopping you. And yet here in the present, one technology in the form of self-checkout machines can be manipulated to defeat another technology in the form of security sensors - which brings us back to the same situation as before! Perhaps no matter how many layers of technology we pile atop our daily lives, at the end of the day our freedom is *ours* to make, and that is the human choice. Keep thinking!

Fun with Novell

by Cronicl3
cronicl3@gmail.com

My school uses a Novell/NetWare network and manages its users with GroupWise. I'd been trying for the past two years to somehow attain network passes. However Novell's password database is quite secure. The main user/pass database on the server is encrypted with some ridiculous RSA encryption and is nearly impossible to get to. However, when users login, their passwords are stored in XP's SAM files. That sounds like a good target. As many of you probably know, there are several programs out there for "extracting" this data. One of them is the ever-infamous pwdump. It has several versions (pwdump, pwdump2... all the way through pwdump6). All of these variations use the DLL-injection method (samdump.dll) under the lsass.exe process. Unfortunately, many of these programs no longer work (and usually crash the machine) because of the various patches and service packs. Even more so, our admins thought they were secure with SYSKEY on the machines, which encrypts the hashes. A tricked-out version of pwdump2 (originally written to run under NT4) that I found seemed to do the trick.

You can locate this version of pwdump2 and several others at http://www.openwall.com/pass➥words/microsoft-windows-nt-2000-xp-2003.

Run pwdump2 through the command prompt and voila! The usernames and NTLM hashes for all the users that have ever logged on to the machine through Novell! (Mind you, our school ghosts all the machines twice a year, so it's only the users that have logged on since the last ghosting). Running these passes through l0pht or another pass-cracking program (I like john the ripper) will give you most of the passes within a few minutes. Some of the "tougher" ones will take a few hours. Inevitably our sysadmins have logged onto 90 percent of our school's machines themselves, so guess who runs our network now? NetWare administrator, GroupWise managers, grading programs, all at my fingertips. However, not being a "cracker" (aka the bad rep that all "hackers" are given), I have not abused this privilege, although the amount of power I have is truly amazing having full read/write access to our file server, our web server, and both our backup servers.

After several days of exploring, I realized that it must have slipped my mind that I had access to all staff email. Why not take a peek, right? As it turns out, perhaps some things are best left undiscovered. Apparently, as Moebius Strip also discovered in his article in 23:2, interoffice romances do occur quite often. As I'm sure you can imagine, all of this new power I had in my hands was such an insane rush and it was quite hard to keep myself from sharing it with everyone I knew. I knew I had to though because as I'd learned from previous ventures, however untraceable you can make yourself or how perfectly you execute your plan, it's always the people you tell that get you caught.

Interestingly enough, one of our sysadmins seems to condemn the use of Firefox (or any alternative browser for that matter), which is odd because I've met many die-hards for Firefox, Opera, or whatever other browser, but I've never met a die-hard IE fan. Guess there's a first for everything. As an April Fool's joke, I made a little addition to the login scripts that removes IE from the NDS "Novell-Delivered Applications" window and adds Firefox to it instead. Both of our admins, who are less-than-intelligent, still haven't figured it out.

Another popular thing that kids fool around with on our network is nwsend, which is like instant messaging through Novell on the intranet. Included by Novell by default, our admins have disabled it. But you can download it free from download.com, etc. I'd think that if they'd just let the kids have it that the excitement would blow over after about a week and no one would care about it much anymore. After all, through the program you can block messages from users, so teachers, etc., can block everyone and not be harassed. I figured I would test this theory out, so I re-enabled nwsend through Novell and, to say the least, my theory wasn't quite right. Maybe it didn't have enough time to mature, but I quite obviously failed to account for kids that have "skills," prime example being script-kiddies that run a program that floods the system with messages and crashes the network. Our admins ferociously locked down the whole network and scurried about trying to figure out who re-enabled nwsend and looked through log files to see who maybe logged in or somehow got their privileges raised. Of course they found nothing. The only users that had logged in with admin privileges had been themselves, so they immediately began accusing each other and arguing, foul language being the primary vocabulary. I love when dumb admins make themselves look even dumber.

On a final note, don't try these methods if you have a somewhat competent sysadmin (hahaha) who reviews the logs regularly. However, if your case is like mine.... What's that I smell? Could it be some badass pranking? I think it is.

How to Build a Book Safe

by c-dollar

We all love *2600* for its highfalutin articles on port knocking, Caller ID spoofing, Walmart self-checkout hacks, etc., but, sometimes we lose sight of the obvious stuff. Sooner or later, the North Koreans or Iranians are going to bomb us. When that happens, how are you going to pay for doughnuts and beer from the 7-11? It'd be nice to assume you have money in your wallet or shoe, but that may not be the case. Where are you going to hide your emergency cash? In a bible? In a shoe? Well, that's up to you; mine will be safely tucked in a copy of *Jane Eyre*, unlikely to be discovered by the invading ground troops.

For hundreds of years, if not thousands, book safes have been used as a way to conceal things. Even though you may not be captive in a state pen awaiting a file stored in a book (or a cake), a book safe may be for you. It's unlikely that a cursory search of your dwelling will turn up something hidden in a book.

Making one is simple and requires less than an afternoon. First things first - acquire the necessary materials:

1 book (preferably hardcover and larger than six by nine inches)
1 bottle of Elmer's White Glue
1 cheap one inch foam paint brush (or, if you're really cheap, a piece of a t-shirt or sock)
1 box cutter
1 Dremel rotary tool (or similar - optional)
1 ruler
1 desire to hide something in plain sight

Regarding the materials, books are easy to come by. Please don't steal a book from the library; libraries are awesome. Go to a garage sale and grab any book of the appropriate size. The bigger the better, and the more obtuse the subject matter the better. Don't pay more than a dollar for the book. Bonus points if you choose a crappy book packed with right-wing politics.

Open the book. Skip the first 15 pages or so. Use your ruler to draw a rectangle you're going to cut out. Keep the rectangle at least two inches from each side. My first attempt failed due to my attempt to hollow out too much of the book. Now I know you all have Dremels that you used to cut vanity windows on your Lian Li cases, but they're not a necessity. A box cutter

or X-Acto knife will work fine.

In any case, choose your weapon and begin cutting on the rectangle you drew. If you use a Dremel, be very careful not to set the book on fire - aim to cut around 20 pages at a time. Hold the Dremel in paper for more than 30 seconds and you've got a fire on your hands.

Once you've completed the first rectangle, pull out the section of pages you've cut. If you're having trouble pulling out the pages, use the box cutter or X-acto knife to trim the parts you missed. Pay special attention to the outer edge of the book; you really don't want to tear those pages or the end product won't look convincing. Repeat until you've hollowed out enough of the book to hold your secret. Patience is a virtue; if you move too fast, you're going to mess up the pages and your safe won't be so stealth.

Once you've hollowed out enough of the book, empty any paper shards into the trash. Close the book and squirt your white glue into a container. Dip your brush in the glue and paint the edges of the exposed pages. Lay the book flat, put something heavy on it, and let it sit for a few hours. Once it's dry, open the cover and trim the edges of the opening using the box cutter or X-Acto knife. Once you have smooth edges, use your paint brush and spread more white glue on the inside of the secret compartment. An hour later, you have your book safe! Now, stuff it with cash, important papers, Dell coupons, or whatever. Rest assured, it will take invading armies quite awhile to find your stash!

Network Programming and Distributed Scripting with newLISP

by ax0n

newLISP (www.newlisp.org) is a relative newcomer to the interpreted language arena in terms of popularity. While it had its humble beginnings back in 1991 when Lutz Mueller started working on it, only in the last four years has development been consistently active.

newLISP is everything that old-school LISP languages are, with a lot of modern features. First off, it's a scripting language that's extremely fast. It has networking ability that's powerful enough to write TCP or UDP client or server applications. Then, to top that off, it has a command called net-eval which makes newLISP stand out from the crowd by giving it the unique ability to easily distribute tasks to other nodes over a network connection.

Binaries (under 200 kilobytes) are available for Windows, BSD, Linux, Mac OS X, Solaris, and a host of other platforms. It is released under the GPL. Performance is also second to none. newLISP has been topping the charts on script interpreter benchmarks in several categories thanks to its small size (under 200 kilobytes) and efficient C code. It outruns php, perl, and even ruby.

newLISP also has some other tricks up its sleeve that make it an excellent system administration scripting language. It has decent filesystem support so it can see if files or directories exist and determine if a file's permissions are acceptable for reading or writing. It has very powerful text processing ability using PCRE (Perl Compatible Regular Expressions). Finally, it's also worth mentioning that newLISP can easily import whole functions from dynamic libraries such as libmysqlclient (instant MySQL access from within newLISP!), tcl/tk (for creating graphical applications in newLISP), and zlib (for compression and decompression) just to name a few. This makes newLISP one of the most robust and flexible languages around.

As you can tell, newLISP is a formidable choice for hackers, geeks, network admins, or security professionals wishing to create scripted programs to do network operations or distributed computing with minimal effort.

I am lucky to have been able to work directly with Lutz, the founder and creator of newLISP. I got a few direct lessons from him and, from there, started tinkering with it on my own. With that, the first thing I did was create a makeshift port scanner. I learn easiest by example, so here is what I came up with.

```
[port.lsp]

#!/usr/bin/newlisp
(set 'params (main-args))
(if (< (length params) 5)
  (begin
    (println "USAGE: port.lsp
host begin-port end-port")
    (exit)
  )
)
(set 'host (nth 2 params))
(set 'bport (int (nth 3 params)))
(set 'eport (int (nth 4 params)))
(for (port bport eport)
  (begin
   (set 'socket (net-connect host port))
   (if socket (println port " open"))
  )
)

(exit)
```

The first part simply assigns the command line arguments into a list called params, then makes sure that four parameters were given (program name, host, begin port, and ending port). If not, it displays a usage tip before exiting.

The second part assigns elements of the list to appropriate variables, then uses a for loop to iterate through the ports, displaying open port numbers that are open. Note that on machines with packet filters that "drop" packets, this port scan will take a very long time. nmap is a much more robust port scanner, however this little script demonstrates the power of newLISP's network commands. We'll run this as a test just for fun:

```
./port.lsp 192.168.0.105 1 200
```

```
21 open
22 open
23 open
25 open
79 open
111 open
```

Now, let's look into distributed computing, shall we? The core command behind newLISP's distributed computing power - called "net-eval" - operates on a list of lists (similar to a three dimensional array). The innermost list is a list of host, port, and a string representing the command(s) you wish to run on the remote node. The outermost list can contain as many host-port-command lists as your heart desires, allowing you to run many distributed processes at once and get the results back all at the same time. Then, outside those lists is a timeout in milliseconds. If a result isn't returned in the timeout period, the operation returns "nil" (that is, false). To clarify, net-eval syntax is as follows:

(net-eval (list (list "host" port-number command-string)) timeout)

On each remote node, you must have a newLISP listener, which is simply started by running "newlisp -c -d { port number" from the command line. On UNIX environments, you may put an ampersand (&) at the end to launch it in the background, or you may even wish to use "set NOHUP" and log off to leave it running in the background indefinitely. In my example, I went to my Solaris box and launched it, listening on port 31337 as follows:

```
$ newlisp -c -d 31337 &
2672
$
```

I also launched newLISP listeners on various other machines on my home network, including a few OpenBSD machines and my wife's MUD/BBS server running Windows Server 2003 with the "Services for UNIX" tools installed.

Now, care must be taken. It is a bad idea to have a newLISP listener running on a public IP address, because commands like process or exec can launch shell processes on the newLISP node, which is just as good as giving away an unprotected shell account on your network. I advise using newLISP listener nodes only behind a NAT or firewall, or on a segregated network.

Let's run a test script, shall we? In LISP, boolean and math operations are always performed by placing the operator first, followed by the symbols to apply it to. In addition, the symbols are numbers, but they could easily be strings or lists with some operations. Adding 1+2 in LISP is as simple as (+ 1 2). I will start by running a quick addition operation on one remote node with a 3000ms (3 second) timeout.

[net-eval-test.lsp]

```
#!/usr/bin/newlisp
(set 'evalstring "(+ 1 2)")
(println (net-eval (list (list
 192.168.0.55" 31337 evalstring)) 3000))
(exit)
```

When we run it, we get the answer to this mind-boggling math problem:

```
$ ./net-eval-test.lsp
(3)
```

Now, to expand this even more, I have added three other nodes into the mix, which shows more clearly how the nested list syntax of net-eval works, and I'll demonstrate remote command execution at the same time, using the "exec" command. Notice how the quotes around the command to be run is escaped with backslashes. This is needed to keep from confusing the interpreter. To put quotes inside a quoted string, you need to escape them. This is almost universal to all programming languages. On UNIX-like platforms, uname is used to get information about the operating system and architecture. uname -s -n -m will list the OS that's running, the hostname, and the machine architecture.

[uname.lsp]

```
#!/usr/bin/newlisp
(set 'evalstring "(exec \
"uname -s -n -m\ ")")
(println (net-eval (list
        (list "localhost" 31337 evalstring)
        (list "192.168.0.55"
31337 evalstring)
        (list "192.168.0.102"
31337 evalstring)
        (list "192.168.0.127"
31337 evalstring)
        ) 3000))
(exit)
```

The result is a newLISP list of strings, containing the results of running the command:

```
$ ./uname.lsp
(("SunOS sparky sun4u") ("OpenBSD compy386
i386") ("OpenBSD bouncer sparc")
 ("Windows mudbbs x86"))
```

The online documentation for newLISP is very extensive and features a few rather advanced demonstration scripts, including a working web server written entirely in newLISP. While learning a new programming language is never easy, newLISP is more than mature enough in both implementation and documentation to make it a pretty easy language to add to your list.

Links

http://www.newlisp.org - NewLISP Website, full of demonstration newLISP programs, documentation, binaries for many platforms, and newLISP source code.

http://newlisper.blogspot.com - *NewLISPer* is a journal, or blog, written by a guy who was just learning newLISP. It's turned into a bunch of newLISP tutorials with some philosophy tossed in as well.

http://www.nodep.nl/newlisp - Norman's code snippets is a website full of newLISP programs and snippets for Linux (not tested on other platforms). There are a lot of really interesting applications and widgets available to download.

Conversati

Suggestion

Dear *2600*:

I've just discovered Revision3 - the online TV station - and I thought why don't you guys at *2600* do *Off The Hook* as a TV show as well? It would just be you guys in the studio talking but you could then edit the video afterwards and throw in screenshots, links, video clips, or something else about the topics you are talking about. I think it would work quite well and I'm sure most of us *2600* readers would love it.

aft

It sounds like a great idea but the problem is that all of these endeavors take a great deal of work and coordination and our time is already pretty stretched to the max. If it's possible to pull something like this off, we'll certainly give it a try.

Reaction

Dear *2600*:

I've been an avid reader for several years now but some things in *2600* are starting to make me lose interest. For example, every commentary I read contains phrases like "George Bush is spying on us" and "George Bush's domestic surveillance program." I am so sick and tired of people repeating talking points from the Democratic Party word for word in their commentaries regarding computer security. Can we stop acting like morons and actually examine these programs without whining about George Bush? Every time I read something from one of your commentators I feel like they haven't even done a shred of research. They simply copy/paste crap from the media concerning the NSA. Last time I checked this magazine was about independent thought, not ignorant political rants. If we want to talk about national security, why doesn't someone mention how George Bush hasn't sealed our borders even after 3,000 people were killed on 9/11? Why don't we discuss real issues that matter instead of constantly whining about the NSA and the "evil" Bush administration? It's getting redundant and quite boring to read in every issue. Can't we be more informed? Don't we have the Internet and alternative forms of media to find the truth and not just repeat what people with an agenda tell us? I wouldn't even mind someone complaining about the NSA if they actually took five seconds to get their facts even remotely correct. This program I read about covers people in America who make a phone call to al-Qaeda overseas. It's that simple, yet we all act like George Bush climbed into our telephones. A well-reasoned argument against the NSA wiretapping would be something interesting to read. I haven't seen anything that resembles a "well reasoned" argument from any article for months now.

comfreak

Believe it or not, this is an issue that affects everyone, regardless of political affiliation. And the wiretapping issue is nowhere near as simple as you make it out to be. We're not about to tell people to avoid a subject that our particular community understands better than most insofar as the threats to privacy and the implications of information gathering. "Independent thought" is also critical thought and never has there been a time where that has been more in need. As for a "well reasoned" argument, let's defer to our readers.

Dear *2600*:

In 23:3 page 37, R wrote about how it's difficult to get friends to care about the NSA's call record database. They give the standard "I'm not a terrorist so it won't hurt me" argument. We know why surveillance like this is a bad idea but sometimes it can be helpful to try to put things in a way that people like that can understand.

The NSA's database is all about datamining and finding connections where they may not have been found in the past. The problem with that is that they'll also find connections that don't exist. R, tell your friends to think about this scenario: you call five friends, and each of those five friends happens to have gotten a call from a friend in a sensitive political region. The feds have already picked your friends up, but they also decide to pick you up too "just in case." Before you can say "Surely there's been some mistake," you're tackled in your own home and lying on the ground with a boot firmly planted on the back of your neck.

Of course, being Not A Terrorist, you have nothing to worry about. Everything will get straightened out and they'll determine that you had nothing to do with terrorism and release you. The problem is they can't "unarrest" you. They won't tell your neighbors that it was all a mistake. They won't make that dirty feeling go away, or the fear.

Maybe to avoid that kind of situation before it happens, you'll change your behavior. You're not a terrorist, of course, but... maybe it'd be prudent to stop talking to your friends in Baghdad just until things calm down. Maybe you'll start being very careful

about who you call in case a spurious connection to terrorism is found. That's what's called a "chilling effect" on free speech, and preventing that is why the freedom of speech is the first amendment.

We *2600* readers know all this and have it distilled down to a few basic axioms like "surveillance is bad," but every once in a while it can be helpful to ground things in the concrete.

Lex

We couldn't have said it better. This kind of thing doesn't just affect those of us who get falsely accused. We all feel it and that gets manifested in how we behave: who we talk to, what websites we go to, ways that we look at the people around us, etc. It's a sickness that has to be recognized before we stand any chance of stopping it. We're impressed with the number of people who get this. We can't allow ourselves to be discouraged into thinking we're powerless to change the direction we're heading in. Nor can we be convinced that this is not something for us to be talking about. This should be a paramount issue for freethinking people in any forum.

Dear *2600*:

In response to the letter submitted by the former NSA employee, from my experience not all of the "phobia" expressed by the *2600* society is "hogwash." In particular, I would be concerned with the monitoring of communications and other activities. As a former employee of a background investigation company called ChoicePoint, I have personally witnessed such activities. As well as other services, we performed background "checks" for the FBI, CIA, and NBA (OK, maybe not the latter). Just before I resigned, the CEO of ChoicePoint approached my team and inquired how difficult it would be to not only monitor the "activities" of someone - let's say an FBI applicant - for their six month probation period, but to monitor the people with whom they associated. To clarify, he wanted to monitor the subject's friends, family, and acquaintances. His justification was "birds of a feather flock together." So if your friend is engaged in criminal activities then you, by association, would be flagged as well. I'll let you form your own opinions regarding the moral issues involved, but apparently the legal issues were not a concern to him. Our mission as developers, handed down directly from him: "not to question why but just to do or die." Hence my departure.

X!U304d

Dear *2600*:

Had to write regarding the disgruntled Cox subscriber (second letter in 23:3). This individual promptly snivels about his privacy after stealing a movie online. Lovely. What "privacy" were you hoping for? Wake up, sheep! You volunteered to use a corporation's server (capitalism rules!) to access the net. You volunteered to abide by *their* "terms of use" agreement. You promptly broke the law. Now you're upset because they monitored your downloads? *You* are the reason they monitor downloads. And you give a nice little blurb - "the movie sucked." Well, that justifies your actions. The movie sucked, so breaking the law and, more importantly, willfully violating the terms of use - a clear cut breach of contract - shouldn't apply to you. Golly, the injustice of it all! All information should be free. Stealing creative works of art is not. You seem to miss something here, so I'll repeat it: You volunteered to use the company's portal to the Internet *under their terms*. Further, "buying" a copy of a creative body of work is not ownership of the copyright as you seem to think. It is buying a license to use - subject to the agreed upon terms. Sharing is good, like you said. Sharing of information, to be clear, is great, and I will vehemently stand up for that. Do not believe that any ISPs are benign in their service. They are justifiably concerned about being an unknowing partner in online crimes. The push behind the monitoring is not moral. It is the team of flesh eating barristers they hire to remain solvent and profitable.

Steve

Dear *2600*:

This is in response to Beowulf's letter in 23:3 which was in regards to my original letter in 23:1. First off, the site that I had found the information on the CEH had a pricing of about $150 to take the exam. I rounded up, and I do apologize. I also apologize for not being clear in my letter about my situation. I am a college student. However, I attend a school that does not offer campus dorms so I am forced to rent. I had two jobs at the time because I needed to pay rent, electric, phone, and all that fun stuff. I was going through a rough time then.

I was using the CEH as an example of my point that there are companies that put things a little too highly priced for people who are in the same financial situation as me to get started easily in this great industry. But now that I actually think about that statement, I suppose it is the same for any industry. I am also learning. I use the articles from this fine publication to expand my knowledge and understanding of Unix based operating systems. I am in the process of teaching myself programming so that I may grasp a better understanding of the various languages that are out there. However, I have always been a fan of study guides.

I see the various certification exams as important building blocks for my future. To me it does not matter if an exam costs $50 or $350. I am spending money to take these tests and I want to pass. So I read study guides and I know that it is not the best way to learn new things. The best way to learn is from experience. I can only gain so much from creating my own study labs. I need experience in the field. And to my understanding, certifications are a huge part of getting into that field.

I have since become full-time at one of the two jobs I was working at and I quit the other to give myself more time for other things such as my girlfriend, friends, etc. I thank you, sir, for your advice and

kind words. It is hard to enjoy learning about how the government came up with laws to stop monopolies back in the early 20th century. But I only have four more months before I graduate with my associates, so I am sticking with it. It's nice to know that people out there are concerned about us college kids. I appreciate it and thank you again. I also say thank you once more to the makers of this awesome magazine. You guys seriously rock!

P3ngu1n

Dear *2600*:

I know this may seem a little late, but I've been meaning to write you a letter and as I was rereading an old issue I thought the quote you opened with in issue 22:2 seemed a bit misleading. This struck me as odd since most of your issues open with a quotation having very much to do with ethics. I wonder if that quote from Orwell, "Men are only as good as their technical development allows them to be," might have been taken out of context in a way. Did he not mean by "good" that they are merely as technically "capable and productive" as their technical development allows? Either way, that would make much more sense because technical development has not at all seemed to improve the moral or ethical character of mankind. And that brings me to the crux of my position which I have wanted you to respond to for some time. The technical capabilities of hacking computer technology may be amorally used for good or evil, but the evil which you seem to often downplay can be of devastating power and seems far more insidious as large bureaucracies make use of technical capabilities to further their agenda. In regards to that point about power I'll point out that as our lives become more dependent upon computer technology a single person acting destructively can cause far more damage. And the information, which the hacker credo suggests should ever be free and available to all, might bring about great devastation. I can think of a number of weapons technologies, for instance, whose technical schematics ought to be hidden if not destroyed. Of course, technical capability grows and, sooner or later, these devastating technologies will become practically commonplace and, inevitably, put to use. Men are indeed only as good as their technical ability allows them to be. Now I realize that your staff has spent their lives improving and believing in the neutrality of computer technology, and I don't criticize that behavior simply to be mean, but how neutral is it when an individual can obtain highly destructive information and corporations use the ability to promote the highest level of ecological consumption in the history of civilization? As much as the technology might help one individual find some sort of zen happiness, how many millions of others does it simply compel to shop? Are the benefits brought about by easily accessed knowledge about, say, the environment, offset by the environmental harm caused by the consumerism enabled at the same time? That's to say nothing of the harm directly caused by the manufacture of computer related equipment. And so this is my sincere and honest critique which I challenge you to answer. My conclusion, paradoxically, is that the greatest use of computer technology is against itself, which I hope this message serves to do.

An Unapologetic Neo-Luddite

Information will eventually fall into the wrong hands. This is as inevitable as the sun rising. And it's certainly true that we've come to rely on technology to such a great extent that it's easier than ever to uncover vast amounts of personal data and create massive disruptions with the same amount of malice that a few decades ago would have been sufficient for a childish prank. While many feel the solution is to forbid any sort of tampering which could result in something catastrophic, that doesn't solve the bigger problem which is the overall insecurity and lack of forethought in design. We can't blame this on the computer technology itself but rather on how we choose to interrelate with it. If we become enslaved to a technology, that's a human issue that we need to address, not a technological one. If "highly destructive information" is stored on computers, that doesn't make the computer any less neutral. Rather, it speaks to our motives and failings as humans and that's where the attention should be focused. Great good can come from technology as well as great harm. It's our choice how we use it. Eventually the system will fail for one reason or another. And we cannot be so dependent on our technology that we don't have a plan for when that happens. Weapons technology is something of a parallel as we see such "advancements" now being made in other parts of the world, something that would have been unthinkable not too long ago. The fact is that the genie cannot be put back in the bottle once it's out and eventually someone you're not comfortable with is going to gain access, more times than not legitimately. Regardless of how you feel about technology, pretending it's not there, hoping it will go away, or forbidding it from being tested and abused only puts off the inevitable.

Oppression

Dear *2600*:

Check this out! We got peaceful hippies, right? No weapons whatsoever. And what happens? The government comes after us with M16s! I am not much of a writer, so I'll just give you this link: http://www.➥youtube.com/watch?v=1hAx5G0I9mU. The movie is pretty much self-explanatory. We need to get the word out. The more people know what is happening, the better. This falls right along the lines of what *2600* stands for. Hackers stand for freedom. Every freedom enumerated in the constitution including that of the right to assemble peacefully, as is evidenced by HOPE and various peaceful protests carried out by its members and readers. I myself am a reader. Yep, that's right, a hippie that reads *2600*. OK, I'm gonna stop right there before I go off on a long rant. Enjoy the rampant display of violence towards peaceful

people, and the wonderful way in which we overcome the violence!

Kevin

With the exception of the cameraman's mutterings, this seems to be a peaceful group confronted by a bunch of confused and overarmed cops. Fortunately this episode ended well. One of the better things to come out of our surveillance society is the ability to surveil right back in the faces of those in power. When the authorities do something out of line, you can count on someone in the vicinity to capture it all and share it with the world. It doesn't change the fact that we lose more privacy on a daily basis with all of the cameras, detectors, and computer analysis targeting us all. But at least we're grabbing a little bit of that to use for individual rights.

Dear *2600*:

Good day all. I am writing this letter in regards to a telecommunications firm whose name will not be stated. I attempted to pay a bill online which was successful. I then called to speak to a "representative." They were not aware that the payment was made due to the fact the system had not alerted them. In order to restore services they *demanded* that I give them a daytime telephone number where I could be reached to get service again. The same person asked me for this three times despite being told repeatedly that this number was unavailable. Then I was transferred to the billing department. The payment was made electronically, which was unknown to the human being on the other phone. What in Ohm's law does my daytime phone number have to do with phone service?

I urge all of your readers to implement a voice over Internet solution and an analog line for contingency purposes. *Down with Analog Service Providers! Keep the Technology, Dump the Monopoly!*

Serkit

This is a common ploy by many companies, telecommunications and otherwise. When they have you on the line, they will try almost anything to get more information out of you. Then they use this for marketing purposes, whether that means calling you to try and market some crap or simply selling your information to some other group of sleazebags. Congratulations on resisting their datamining attempt.

Dear *2600*:

At my work area we use iMac computers. Which I dislike. I dislike these computers mostly for the OS. OS X does not make me happy. We also have to use a password to get past an overly-oppressive security system. The blocker we have is incredibly tight. It will not allow any access to forums of any sort, anything with "profanities" (some of the things considered profanities were words we were allowed to say in Grade 2), and all the other stuff bosses don't like. Early on we found out that the security seemed to work with Safari (OS X's main Internet browser) but not with Internet Explorer. We decided not to go into detail with this because we enjoyed the freedom. However, it was temporary. Eventually the network admins decided to make the Internet Explorer folder admin only and lock it off to us mere mortals. After about a month of suffering under Safari (which seems to be loaded with bugs as well as the blocker) we came upon a fun little way around Safari into Internet Explorer. It's very simple. Go to any application and click Help. It'll open up a nice little window with the OS X logo on the left. Under that will be a link to the Mac website. A simple click and you've got yourself a nice Internet Explorer window. This is a great trick to use if you've got a nasty blocker that only works with Safari, or Safari is asking you for a keychain password every couple of pages. Thanks to the writer of the Windows Media Player window trick for helping us get the idea!

Darkpr0

Of course this little trick is very simple to fix or prevent from happening in the first place. But you have the right idea in resisting this level of control. It's not something specific to the Mac OS however. Blocking software works on nearly all platforms and the better they get the more frustrating it will become for those of us who just want to be left alone.

Dear *2600*:

It looks like Visa is taking the first steps to demonize the use of money in their current commercial. They apparently don't want us buying things that can't be traced back to who bought it and when. If this line of advertising expands, soon if you pay cash you will be looked at suspiciously. I know some work has been done on this, but someone has to get a form of anonymous card money out into the mainstream market.

Thanks for all the good work that you do.

Barada

People who pay cash are already looked at with suspicion in many areas. Airports are only one example of this. The commercial you refer to shows a busy deli at lunchtime where everyone moves at an astonishingly efficient pace until some poor guy tries to pay with cash instead of plastic. The resulting bedlam ends in the complete breakdown of the system. What's most humorous about the whole thing is that the people running this ad campaign probably never thought anyone would draw inspiration from the chaos they illustrated. Efficiency is all fine and good but the insane pressure to conform and the monitoring that goes along with that are not what healthy individuals crave. We encourage people to use cash whenever they can, even if it's only to make a point.

Dear *2600*:

I recently started reading *2600* and I especially like the articles about privacy and electronic security. It's a shame the direction this country is headed towards, and unfortunately our elected representatives have so far been total failures at keeping up with privacy in the information age. Many of the worst offenses have been perpetrated by those who are supposed

to be working to protect our rights, not violate them and put us all at risk. Many people probably know that you can do background checks on people at pay websites, but now many states are putting even the most trivial of offenses - such as traffic tickets - online for everyone to see. At mdcourts.gov, for example, you can search by last name or last and first names to find cases including any traffic tickets in the entire state of Maryland. The results include the defendant's full name, full address, driving license number and state, month/year of birth, height and weight, and vehicle tag number, in addition to the fine and disposition. I often check this on people I date, mainly out of curiosity to see what they've done and to see what their age is. Of course, most people have no idea how dangerous it is to give out your real first and last name, so it's easy to look them up and certainly more than half of them have had at least one traffic ticket. Virginia also makes this data available online and they give the month/day of birth, so if they have a ticket there as well as in Maryland, it's easy enough to put together the whole date of birth. Of course, you can also just drop into the local courthouse and look at the actual citation, which they keep on file forever and is open to the public. This often contains the Social Security Number. As you can see, this is everything someone needs to commit identity theft or stalk an ex-lover. Moreover, since the information is probably available in electronic batch format and sold to make the states money, it can be used for targeted advertising, collections, and so on. To be honest, this most trivial of information is much more than cops in most jurisdictions get while doing a traffic stop and entering your data into their car computers. I honestly see no reason why such detailed personal information needs to be made available by state courts online. There's no administrative reason to make it available and even if you think traffic tickets should be public there's no need to include addresses and dates of birth. I personally think criminal records should be nonpublic except for serious offenses where there is a public interest at stake. To blindly make every little detail freely available on the web is the equivalent of putting the whole DMV database online.

JasonB

We'd like to know if anyone has ever been caught giving a false Social Security Number when getting a traffic ticket. Obviously if it's already printed on your license, you would have a tough time pulling that off. Otherwise it seems an almost necessary step to protect at least one important part of your privacy.

Submission

Dear *2600:*

I sent you an article and wanted to inquire whether you received/looked into it. It's been a while (6/26/06).

Sandro

When you send us an article (at articles@2600.com) you should receive a confirmation email. If you didn't send your article in ASCII text, we suggest you resend it to meet that standard. In all likelihood you won't get a second confirmation email. This is to avoid mail loops and other annoyances. Within a month or so (sometimes longer if we're swamped), you'll be notified if we intend to use it in a future issue. When it does go to print, you will receive a final email requesting info on where to send your free stuff. If your article is not accepted, you won't hear anything after the initial confirmation. Rejection letters result in people wanting to know exactly why they were rejected, prolonged discussions, arguments, blood feuds, etc. If you haven't heard anything for several months after you send in a submission, then you can assume it's not what we're looking for. But don't let that discourage you from submitting something else. As always, we ask that your submissions not be previously printed or available on the net before they're printed here. And if you want to send things snail mail, our address continues to be: 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

Dear *2600:*

What about my proposal of article? I have sent you this proposal some months ago - but I didn't receive any reply. Would you let me know if you think to use it?

Riccardo

We generally don't respond to proposals except to say that if you think something would make a good article and you've read our magazine before, then by all means submit it. It would be unfair of us to tell you subjects that are off-limits. Anything can appeal to the hacker mentality if approached from the right angle. Simply ask yourself if this is the kind of thing a reader of ours would appreciate and whether it's different from what you might find in another magazine. So the short answer is: Send it in! Even if it doesn't run in our pages, you've still created something new and that opens up all sorts of possibilities.

Dear *2600:*

I have written an article that I am interested in publishing anonymously. I do have some concerns over the protection of my identity should the company I am writing about demand it of you. I have been a reader for about eight years now and would never have considered writing the article to begin with if I was not confident that your organization would keep my identity anonymous, but I guess I am just looking for a little reassurance before submitting it. I have sought legal advice on the topic and was told that *if* the company were to invest in identifying me and *if* they were to successfully identify me they *might* have a case for revealing corporate secrets. To be honest, even as I am writing this I seriously doubt this particular company would care to invest in finding me.... Then again....

Also, I know there are no strict guidelines for article submission as far as length, but my article is a

little over 2000 words. Is that cool?

Name Removed

First, we sure hope that wasn't your real name you used in that letter if you're this worried about keeping your identity secret. We can keep our mouths shut but many others can't. In all of the years we've been publishing, we have never given out the name of someone who didn't want their identity revealed. There have been unfortunate instances where information in the name someone used was enough for their employer to track them down and take action. That's why it's so important to not give away details of your location, name, appearance, or anything which someone could use the process of elimination in order to come knocking at your door. We take confidentiality very seriously, even if other members of the media don't. But you also have to take precautions on your end, such as not submitting something under the same username that people already know you by. If you wish to remain anonymous, just say so and we won't use any name at all to identify you. But even this may not be enough if you're sending email from an insecure location, such as your school or workplace. As for length, that's not something to worry about if your subject matter is interesting, which we suspect it is.

Question

Dear *2600*:

I recently purchased the latest issue of *PC Magazine* titled: "How to Hack Everything." I was very disappointed, however, when I could not find information therein on how to hack a Gibson. I was told that if I want to be elite, I have to do a righteous hack on some heavy metal. How can *PC Magazine* get away with leaving out such valuable information?!

vyxenangel

The only way to get the mass media to print the specific info you require is to deluge them with requests and demands for it. Tell them you will file them under "garbage" if they don't listen. That usually works.

Dear *2600*:

I am the librarian at DeVry University in Tinley Park, Illinois. One of my student workers subscribes to your magazine and he showed me an article, "Hope and Fear," that was published in 23:3. I think it is a well reasoned, well written article.

A few years ago some students from DeVry went to Defcon in Las Vegas. I went as an "advisor" for the group. I must say that it was quite the culture shock for me. I presumed the seminars would be all technology-based programming, circuits, etc. The discussions included, among other topics, free speech, intellectual freedom, and intellectual property. I must say I was very surprised. Many of the issues discussed were issues that I deal with as a librarian. When I told people that Defcon is a hacker's conference they always wanted to know why I wanted to hang around "people like that." The "cracker" versus "hacker" lecture then follows. I discovered there is a lot more common ground than meets the eye if only one looks for it.

I teach a course entitled "Critical Thinking and Problem Solving" (I call it "Reasoning and Research"). Among the points I try to emphasize heavily in the course are that there are two sides to every issue (e.g., use of technology) and you need to take a reasoned approach to your life.

The "Hope and Fear" article, I think, expresses these ideas very well. As a result, I would like the (unnamed) author's permission to use the article in class.

Paul Burden

Perception is a funny thing. We need to spend a good deal of time dispelling a lot of myths that surround the hacker world. Such assumptions prevail all around us and we need to seek them out and expose them whenever possible. As for using our article in your class, you're most welcome to. We only ask that you let people know where it's from.

Dear *2600*:

In the Winter or Spring 2006 issue you printed an article or letter that mentioned probability formulas to reduce least likely numbers from Lotto selections. Someone stole my issue.

I would like to try implementing the formula in other areas. The article mentioned the formula was advertised in the classifieds of a major magazine, but did not say which.

Would you tell me the author of the article in your magazine or ask him/her what magazine and issue did the ad appear in?

Greg

The article appeared in the Winter 2005-2006 issue. We're not sure that it would do you much good to know which specific tabloid the "Lottery Secrets Revealed" information was advertised in, especially since the story took place 12 years ago. If we receive more specific info, we will share it. Otherwise you should be able to find all sorts of information (good and bad) by simply searching the net.

Dear *2600*:

Do you guys print any *2600* stickers? It would be nice to be able to slap the name across my laptop to make my interests clear.

Idgeitman

We had stickers for HOPE Number Six which were given out at the door and we have leftovers which we're sending to anyone who orders HOPE shirts off our website. A generic 2600 sticker is something we'd like to consider.

Dear *2600*:

I've been reading your great magazine for about 11 years now. After so many years and still seeing your ads for ordering back issues it has got me wondering. How is it that after 22 years you still have back issues

for every magazine printed? Where do you store them and how much space do they take up? What do you do to protect them from damage? How many copies do you have of the 1984 issues?

E1nstein

We believe it's very important to keep things from going out of print which is why we occasionally have to reprint some of the really old issues. The not-so-old ones have enough extras to last a very long time. But if those should run out and people still want them, we'll reprint those issues as well. We keep them in a safe, dry place with lots of room. And we have lots of 1984 issues since those were just unbound sheets of paper. We only printed a few dozen that first year and we've had to reprint them many, many times since.

Dear *2600:*

So I'm just taking a shot in the dark here but are you guys named after the blue box and its 2600 hertz sound waves?

Clark Milholland

You need to shoot in the dark more often. That's precisely it. To us, 2600 hertz represented the seizing of technology for individual use and abuse. The rest is history.

Dear *2600:*

I am an independent software consultant based in India. I want to reprint *2600: The Hacker Quarterly* and distribute it here in India and would like to know what the options are. The average IT magazine here is sold for one or two dollars.

Raj

We are not opposed to such a venture but it would take a lot of coordination as there would be virtually no way for us to do any of the work in the States without losing a ton of money. You're welcome to write to us with more specifics and the like.

Dear *2600:*

I heard through the rumor mill that passport covers to block RFID signals were handed out at HOPE to participants. Do these passport covers exist? Where could I get one?

Squealing Sheep

One of our vendors (DIFRwear) was in fact a seller of such RFID blocking passport covers as well as RFID blocking wallets. You can visit their site at http://www.difrwear.com.

Dear *2600:*

I have a fourth generation iPod. My battery was running low and I pressed a random sequence of keys on the click wheel. A menu came up in standard text. The menu had the following choices: *"batt a2d, a3d stat, firewire, hdd r/w, smart dat, hdd scan, read sn, diskmode, wheel, contrast, audio, status, drv temp, iram test, 5 in 1, reset, key, chgr curr, remote, hp status, sleep."*

I was going through the menus and then my battery died. Has anyone ever seen this before? And what does the menu do?

Oral Seymour

Dear *2600:*

I am a huge fan and I was wondering if you could tell me about a website that could give me good free music without using Limewire or Kazaa.

Pac.Man

The best method of sharing music is through a group known as Friends. They are quite open to passing around any music that you may find interesting and it's a remarkably easy group to join. What's more, they've been doing this for as long as recorded music has existed.

Dear *2600:*

May I have some shout outs in the next issue? DoofMasterZ, t0mtwinkie, joel, witeboyshuffle, cry.sys, and d/\n. Thank you.

Samuel Reed

Did you grow up in a barn? Shout outs are not something you can just write in and request. They must be earned. So the answer is no, you may not have the shout outs listed above. Respect.

Prosecution

Dear *2600:*

I was wondering if you could possibly give me some advice. Last December I received a letter in the mail from the RIAA asking for a settlement of $4,225.00 for illegal downloading found on my IP address. I then got an attorney and hoped for the best. They are now demanding the settlement or they intend to file suit against me. Is there any way to get out of this? If you have any advice or information that would help me out please write back very soon.

Kristin

It depends on what you want to get out of this. If you want to fight them, then you should. It's very rare for these entities to insist on a settlement if they think they just detected a violation for the first time. It's likely just a scare tactic since taking you to court is expensive and risky for them as well. Regardless, their accusing you isn't enough on its own. It's relatively easy to hop onto an IP via a WiFi link or even by spoofing the address. The burden of proof is on them to prove that it was actually you who did this. Your attorney really should have told you all this.

Dear *2600:*

The Swedish High Court has acquitted a 29-year-old male for sharing files over a P2P network. The reason was that the only "proof" available were screenshots, which the court says is not enough.

Finally! I've heard of many being convicted thanks to screenshots and I got horrified each and every time. Screenshots aren't proof. Those screenshots could easily be fabricated or simply be from an entirely different computer. Just wanted to share what I see as very good news.

aft

Keep in mind that this instance of justice occurred in Sweden, which is about as likely to have an effect on the U.S. judicial system as Pluto.

Revolution

Dear *2600*:

I possess a great fondness for obtaining knowledge and executing creativity. Though my interests stretch wide, my main interests are mathematics, physics, electronics, and of course computer science. I am currently 19. Around the time period my age morphed to 18, I contained a paranoia that disabled me from creating and experimenting. This time frame was terrible. I viewed an extremely corrupted society, a society where humans were sued for creating software that fell under a useless patent, a society where curiosity was frowned upon, etc. I am slowly fighting this evil paranoia and continuing my previous events.

I was inspired to produce this letter after reading the following section from the "Congressional Testimony of Emmanuel Goldstein" on totse.com:

"I would like to close by cautioning the subcommittee and all of us not to mix up these two very distinct worlds we are talking about, the world of the criminal and the world of the experimenter, the person that is seeking to learn. To do so will be to create a society where people are afraid to experiment and try variations on a theme because they might be committing some kind of a crime, and at the same time further legislation could have the effect of not really doing much for drug dealers and gangsters, who are doing far more serious crimes than making free phone calls, and it is not likely to intimidate them very much."

We need a *revolution*.

aRevolutionist

It was almost as if Congress was given a road map of what not to do which they then decided to do anyway.

Clarification

Dear *2600*:

In reference to sc's letter in 23:2 I would like to help out all the musician hackers amongst us who would like help tuning their instruments with more than just an "F". Actually, all over the world the concert tuning note is "concert A," which converts into 440 hertz. Most symphonic orchestras keep increasing this standard tuning note due to an increase in relative brilliance of sound, especially American orchestras. To make a long story short, luckily in the western world (meaning west Europe) you will find an 880 hertz dial tone. So maybe if there are any more variations of dial tones in some deserted parts of the world, guitar players will be able to tune all of their strings without even using their ears. What a bummer that was anyhow!

jazzlup0

Duly noted.

Dear *2600*:

This is in response to lup0's letter in 23:3. This is a possibility since I had a similar experience and I am assuming this since you listed the ports as being 6881-6999 which are BitTorrent ports. The company that owns the copyright material may have actually tried to download the shared copy from you and sent your ISP a Cease and Desist letter or maybe even an email.

The Joker

Dear *2600*:

In response to lup0's letter in 23.3, I would like to point out that in fact Cox is not monitoring the connection's packet payload, but merely the amount and type. I am not defending Cox in the least right now. They are monitoring (I've been shut off before for hosting http services and being one of the reasons they disable hosting on port 80). However there is one thing that lup0 forgot to mention or didn't read. The email he was sent should have very specifically mentioned which *files* he was infringing with, his IP, the time, and the protocol he was using to transfer. All this actually comes from an authorized representative of the movie company. lup0 was not caught by Cox; he was caught by the movie company.

Here's the trick, just so you know: They (the movie company's hired spies) share the movie themselves after they download the pirated copy from us (the people), check it, verify it's the actual movie. These movie companies are *paying* people to share the movies and write down our IP addresses, time, date, files. Here's my workaround: In the email that I received, they (the movie company) requested that the offending files be removed from my system. All these were .R## file parts. They never said anything about what was contained within them! So I unpacked, burned to a CD, put on the network drive, and kept a copy of the AVI (remember, not listed as offending) on my computer, and did as requested. Here's sticking it to the movie companies' bad movies, sharing spies, and stupid lawyers for their awful wording of the email, and forgetting to list "And contained data within listed files."

Cynagen

We suspect they were most interested in you removing the files from public access, not whether or not you held onto a copy as a souvenir.

Dear *2600*:

In regards to lup0's letter in 23:3, the ISP is likely telling the truth. I work at an ISP and occasionally we receive abuse complaints. These complaints detail a time and IP address, and indicate that the user of that IP at that time was "doing something bad" (they give details). In most cases, it's just an infected box probing ports or participating in a DDoS or something. However, once in a while, the IP address and time arrive with a description of a copyrighted work or piece of software that was allegedly being infringed. I believe it works like this:

Copyright holder (RIAA or MPAA or MS) or someone they hired tells the intrusion detection group of the infringement. Intrusion detection group tells the ISP. ISP takes action or ignores it.

The ISP's motivations are presumably just keeping their bandwidth bills manageable. The interesting thing is that if the ISP is not actually invading your privacy, they are taking your accuser at their word, likely without any evidence except for possibly large bandwidth usage. It might be interesting to ask the question: Can an ISP legally take action against you based on the second- or third-hand word of a copyright holder? Should they be able to?

G

Dear *2600:*

In 23:3, lup0 wrote about his ISP blocking Internet access due to file sharing and being able to name the files that were being downloaded, but still saying they do not eavesdrop on their clients' traffic. Quite understandably, lup0 experienced some doubts about this. As I work at an ISP abuse desk in Europe, I believe I can shed some light on what happened.

In 1998, the United States Senate passed a quite strict copyright law called the Digital Millennium Copyright Act (DMCA). Title II of DMCA, the Online Copyright Infringement Liability Limitation Act, creates a "safe harbor" for online service providers against copyright liability if they adhere to and qualify for certain prescribed safe harbor guidelines and promptly block access if they receive a notification from a copyright holder or their agent. What this means in practice is that unless ISPs act when they are notified of copyright violations, they are also held liable.

Some large copyright holders (typically media companies like Universal Studios, Paramount, Sony Pictures, etc.) have hired the services of a company called BayTsp in Los Gatos, California. BayTsp runs computers on DC++, BitTorrent, eDonkey, etc. networks, listening to traffic and noting sharing of items owned by their clients. They then contact the ISP with the information, which includes time stamps, file names, sizes, protocols, and IP addresses. Some copyright holders do very similar things at their own operation.

Thus, lup0's ISP probably didn't eavesdrop on their clients and are forced under very severe penalties to take the action they did.

In the country where I work, privacy laws currently prevent us from having to hound our clients in this manner, but this may change in the future since similar European legislation (EUCD) has been passed. I recommend consulting Wikipedia which has quite good articles on these laws.

Eric Smith

Dear *2600:*

I feel I should reply to a couple of the letters in 23:3 as I work for an ISP and have the ability to answer these.

The first of these was a letter sent in from lup0 where his Internet provider (Cox) had suspended his Internet access for downloading. He was concerned that his provider is monitoring every packet he sends out. This is hardly the case. In situations where people download using Torrent systems or P2P systems without masking their IP somehow, the MPAA or the movie's producers will occasionally send a letter to the ISP stating that "the user with this IP address was downloading this file (e.g., *Mission Impossible 3 - DIVx.AVI*) at this time. Please take action to ensure that sharing of this file by this user is stopped. Thank you." It's been a little while since I've seen one come in so they might not be as vigilant about it anymore.

The second letter I wish to respond to was someone in the UK who had ordered a phone line and DSL, then canceled his phone line and remained on DSL. I know here in Canada where I live things may be different but how it works is our telephone companies are incredibly lazy. The analog signal (voice) on your line can be turned on and off at the flick of a switch essentially. The digital signal (DSL data) however is not as easy to turn on and off. The phone company physically has to add and remove a card in the central office every time someone either subscribes to or cancels DSL service. This on occasion has allowed a digital signal to remain active on a dead telephone line for up to a year and a half in my experience.

D10D3

Dear *2600:*

I just finished reading the article "Never Pay For WiFi Again!" in 23:3. The author said that Apple removed the ability to change one's MAC address since Jaguar. This is not true but they did make it a bit harder. There is a simple program called SpoofMAC that will spoof your MAC address properly with 10.4+ PPC machine airport extremes. I am not sure if this will work on Intel machines. If you prefer the old fashioned way, a Google search will show you how. To any other Mac users who found this article interesting please stop by #kismac on freenode.

BugDave

Proclamation

Dear *2600:*

I am a *patriot*. I send info and bucks to people in the gulag. I do not know how to type and therefore cannot hack. But I'm very interested in acquiring any and all information I can on all subjects. Knowledge is power. If the sheeple believe that their elected officials have their best interest at heart, then let them follow the Judas goat to slaughter. The truth is that you *get* the government you *deserve!* If you will read the constitution of the United States you will see that our founding fathers declared that we were born with certain rights that under no circumstances can be revoked. Yet they continually chip away at these rights. One right is the right to keep and bear arms. This has nothing to do with hunting and everything to

do with overthrowing an oppressive government! They have now enacted laws that give them the authority to come and confiscate your guns if someone merely puts a restraining order on you. This means that they don't even need evidence of a crime, much less a conviction! So I call upon those who have eyes to see and ears to hear to withhold revenue from the scumbags any way possible. Be it getting free stuff or services from the big corporate institutions to not reporting income or even destroying their databases!

Candycone
South Dakota

We're not going to be starting a Second Amendment interpretation discussion here. But if you believe what you say, when exactly will you be using your guns to help overthrow the oppressive government which you obviously have strong feelings about? If that's what they're supposed to be used for, when does the overthrow start and who decides? We admire people who stand up for what they believe in but you seem to be using your dissatisfaction as an excuse to steal and cause havoc without a clear objective. What good will come of that?

Information

Dear *2600:*

Check out http://irrepressible.info - a campaign against censorship on the Internet. And the fact that Amnesty International is leading the campaign actually gives me hope that people just might start to listen to what a lot of us has been shouting for so long.

Anders

Dear *2600:*

Hello my brothers and sisters of the digital underground. I am writing this in response to a previous article or letter which I read in another issue but unfortunately that issue is floating around my personal library somewhere and cannot be found. The article I'm referring to actually talked about using 711 or relay calling to make collect calls from prison. I thought this was interesting because it's kind of crazy what they charge the families and friends of the incarcerated. I hear that prisoners sometimes have access to computers that have active Internet connections. If this is true they could easily create an AIM (AOL Instant Messenger) screen name and add the screen name MYIPRELAY to their buddy list and use the relay service to make calls to whomever they needed to. This not only allows you to make calls at times you might not normally be able to, but it avoids incurring any collect call fees. After adding the MYIPRELAY to your list you can type in the following: dial xxxxxxxxxx. Replace the x's with the telephone number you're calling and the operator on the other end will make the call for you to the desired party. Now if the facility the prisoner is in blocks the AIM Express website, it's time to use an old workaround, a proxy server such as www.proxify.com or www.thecloak.com. Since these prison systems may not allow users to install .exe files, I would suggest using the AIM Express website to login. Plus there is a hack to add AIM contacts to your Gmail Gtalk list since they both use Jabber logins. This is just a random thought from someone who works tech support for a living and is unhappy with the current political condition and hopes that it will save some people some money from the very greedy phone companies. The Gtalk hack can be found in a book entitled *Googlepedia*. Enjoy and happy relaying!

soursoles

While we think it's a great idea, we know of no prison that actually allows its inmates this kind of access on the net. It would certainly make the Internet a much more interesting place if they did. Regardless, something needs to be done about the horrible ripoffs prisoners' friends and families must endure at the hands of those phone companies which charge exorbitant collect call surcharges. Communications costs have gone way down across the board. It's unconscionable that rates many times higher are being charged to those who have very little choice in the matter.

Dear *2600:*

I did some work with a local telephone PBX installer and noticed the tech dialed "10111" on their buttset to give the phone line the tech was connected to, aka dialed the ANAC. I tested this here in Maine and it works only on Verizon landlines, not on Verizon payphones.

Hawk82

Dear *2600:*

Check out this pay service - http://www.spoofcard.com/ - call through them via PIN and you can enter any number you would like to appear as Caller ID and choose a different voice for yourself. Hmmm... the possibilities!

Doda McCheesle

This was demonstrated on "Off The Hook" some months back and has provided many hours of entertainment ever since.

Dear *2600:*

First keep up the awesome publication. I read it to stay sane.

I was frequenting one of my favorite forums when I happened upon a link to http://www.privatephone.com. This intrigued me beyond belief. The way it seems to work is that you choose a state, an area code, and then a city. It'll generate a number for those specifications and then all you need to do is provide a valid email address for this messaging service to work. This seems extremely interesting and looks like a lot of fun could ensue, especially along the lines of remaining anonymous in this day and age when that's becoming increasingly harder.

I wouldn't mind some more information on this service if anyone out there knows anything about it. And I certainly hope I'm not poking at something that has already been discussed. Though I don't believe

that I am.

Crapinaple

These services are popping up all over. The result is a phone network that has almost no similarity to the one where geography actually meant something. Now we can each have dozens of phone numbers from all parts of the country and confuse the hell out of people who want to know where we really are.

Dear *2600:*

I did a bunch of favors for some of the guys at work and they wanted to take me out for lunch. They let me choose the place. I chose a strip club that actually has pretty good food and, of course, good scenery. Looking at the food menu I noticed that they had a website and a section where for a price you can look at the girls in the locker room via a webcam (no sound). I found an unsecured way to access it without even having to get on their website.

My question is whether or not this would be something that you would like me to write about and post the mms address? If not, I can send you the three webcam links for your personal enjoyment.

Also, I have an entertaining story about my ex-girlfriend who I built a computer for (special computer with spyware installed). I found out about her cheating on me with a very well known Hollywood movie star. (Hint: he is known for a very expensive flop that cost about 180 million dollars and was about water.)

Jayster

The webcam thing isn't exactly the hack of the century but if you can put together an article that details how you were able to track down the alternative method of access, it could certainly be useful for many different applications. As for the spyware story, perhaps you could outline how your ex-girlfriend might have been able to get around your surveillance if she suspected that you might be onto her. Some of our readers would like to continue cheating on their significant others without having to worry.

Observation

Dear *2600:*

As always I wait the months for your magazine to arrive and then within a couple of days it's over. This time I have something to contribute.

I work for Telus Telecommunications in BC Canada. I am a service tech doing installs and repairs. A while back I had a job to go to a customer because they couldn't get their ADSL to work. Now the customer had just bought a new computer from Staples and Telus had hooked ADSL up in the CO, so normally there shouldn't be a problem. The customer is given filters for their phones and an instruction CD for software installs and setup.

One thing they have to do is register their MAC address with our OCA server. This customer wasn't able to do this and took the computer back to Staples, which was an hour's drive from the town they lived in.

When I got to the customer's house I didn't have any trouble registering their MAC addy or being able to surf online. The customer was happy and I left. The next day I got a call back. They couldn't surf. After playing around checking the settings and not finding anything wrong, I called our support group to see if something in the software was changed. Lo and behold we found that the same MAC address was registered in another part of the province.

Now we all thought that every MAC address was supposed to be unique. I instructed the customer to take the computer back for a new NIC card. They were told that the computer would have to be returned to HP for the change to take place and instead sold them a router. The router solved their problem and they were again happy customers.

I am guessing that this was a unique and one time error or that the NIC cards were coming out of a country new to this type of marketing such as China. I'm not sure what the answer is but it was a fluke that the support tech decided to look up the MAC registration because they normally don't look that deep or far.

Adelain

Dear *2600:*

I have a little story about the Manchester (New Hampshire) Police Department.

About two weeks ago the local chapter of Easter Seals NH was having an ID Card Night for kids with ASD and PDD (Autism Spectrum Disorder and Pervasive Developmental Disorders). My son is mildly autistic (maybe he will crack the NSA's encryption code!). Anyway, there was a nice policewoman who took us out for a little tour of the police cruiser. I was watering at the mouth - police radio, police radar, and, most of all, onboard computer! As far as I could tell (hands-off of course), I think its OS was either Windows NT Embedded or Windows CE 3.x (looking at the interface). More than likely NT Embedded.

Now for the fun part. I said to the nice policewoman, "Hey, can we see the computer? My son loves computers." "By all means," she said. She pulled the stylus out of the holder and tapped the screen. The screensaver went to the standard Windows logon screen. The username was simply "mpd" (Manchester Police Department, I assume). She left the password blank and hit the "logon" button. *Wow!!*

The interface came to life. On the screen was an interface for *anything*. You name it. Driver's license lookup, license tag lookup, GPS coordinates of the cruiser. The information! I actually had to keep my hands at my sides, it was so tempting. Now what really frightens me is that the car was unlocked and out of view. So what was to stop anyone with half a brain getting all of the juicy information that Big Brother had?

So much for security.

Zaphod

We imagine even half a brain would be sufficient to steer someone away from messing with a police car. We wonder what checks and balances are in

place to prevent abuse of this system by both authorized and unauthorized parties. Imagine a cop who's also a stalker and the risks become all too clear.

Dear *2600*:

I recently did some traveling in Japan and I was struck by the differences in airport security there versus here. The security officers in Japan clearly took their job seriously and didn't appear both in physical appearance and body language to have made the choice of working airport security over working at McDonald's. What was most immediately obvious was the number of X-ray machines. I had traveled through both DFW and LAX on my way to Japan and neither airport had more than two X-ray machines operating at any time resulting in a huge line, frustrated passengers, and overworked guards. Japan had nine X-rays going at all three airports I went to there. But the most intriguing thing I saw that prompted me to write this letter was a liquid testing machine they have. They allow passengers to take liquids on flights domestically and internationally unless that travel is through U.S. airspace. They have a machine that is about 18 inches tall and has two C shaped openings. At the base of these two openings is a metal plate of what looked like tin. I placed my drink on the opening for plastic bottles (the other is for metal containers) and after a few seconds a green light came on and I was allowed to keep my drink. I wanted to learn more about the device but the only English on it was what appeared to be a company logo with the letters GTC and ironically the on/off switch. As it was explained to us, foreigners have absolutely no rights in Japan so I was hesitant to take a photo of the device. If anybody knows anything about this machine, write an article. I want to learn more about it. It obviously wasn't new so it wasn't in response to anything recent.

GBM76010

Japan is the place to go if you want to see weird machines that know what they're doing. If you just want to see confused people who have no clue what they're doing, a trip to a domestic airport will be most rewarding.

Dear *2600*:

I tried to log onto my Key Bank online account and discovered a new security "feature." All computers logging on now are required to be registered to access the site. According to the representatives I've spoken with, this entails only a logging of my IP address. To register I must provide my ATM card number, PIN(!), and debit card issue number. How many clueless WiFi users are going to have their identity stolen because of this "feature?" There isn't even a warning about accessing account information over WiFi. Why are the people charged with our security always so clueless about what security really is?

Brian

Dear *2600*:

I was just looking through the *2600* cover archive and noticed in May 1987 a plane was depicted flying into the twin towers. It can be seen in the "covers" section of www.2600.com.

By the way, It would be rad if you guys did a retro cover one of these quarters.

knotnaught

We were hoping this wouldn't come up. And now we're probably going to have to reprint those 1987 issues. As for the retro stuff, perhaps in the future.

Dear *2600*:

I want to thank you and Arcade One for raising my sense of paranoia. The other day I went out to get some lunch so, while I was out, I decided to stop by the bookstore to get the new Fall issue of *2600*. After standing in line for 20 minutes due to the incompetence of the bookstore cashier, I found myself rushed to get lunch and get back to work. I decided Panera Bread was the best choice since it was close by and it was closest to my workplace.

I had never been inside any Panera Bread prior to this visit. There were just a few people in line since it was only 11 am. So while I stood there, I pulled out the issue and started to read the article "Identity Theft: Misinformation Can Be Your Friend" by Arcade One. Eventually it was my turn to order, so I blurted out my order and returned to my reading. Then I heard the cashier ask, "What's your name?" I froze. There must have been an obvious, shocked look on my face because the cashier snickered. At first I thought she might be trying to hit on me, but then I realized she really wanted to know my name to complete the transaction. I asked myself, "Why am I required to give my name to purchase a sandwich?" All sorts of thoughts raced through my head and when she asked the second time I knew I had to say something, because by that time people were starting to get in line behind me. So, in desperation I pulled out a hack I had used for years against Radio Shack. I lied and said my name was Mike. The cashier entered the data into the computer/cash register and handed me my ticket. The name "Mike" was printed on the receipt next to the ticket number.

My heart was actually racing as I stood by the pick-up area of the counter. What if they asked for ID to prove that I was this strangely behaving "Mike" who had ordered this very sandwich in question? What if another Mike, or God forbid, two Mikes, Mikes who had told the truth, had gotten in line behind me and were now approaching the pick-up counter? What if they took my sandwich? Would my sandwich die because I lied?

After a few minutes I heard a call for "Mike!", so I grabbed the food, just glad I had asked for it "to go." As I opened the door I felt this rush of adrenaline, as if I had committed some crime and gotten away with it. By the time I got back to the car the rush disappeared. I realized that Panera Bread was probably using the name method to keep from mixing up the orders or personalizing the experience, but then wouldn't the unique ticket number suffice? I also found myself wondering what happened to that

data the cashier entered. Did it go to a central server? How long would it be kept? What if I had said my name was Osama? What if I had refused to give a name? I think what I should have done was to have asked why they required my name at all, but I was too embroiled in conspiracy theories to have thought of that option. However, you might want to try it for yourselves, *2600*. I'm not sure if they all do this and I won't say which one it is, but the Panera Bread store I visited is less than 15 miles from the St. James, New York address you list in your magazine.

Mike the Liar

We detect what may be a tinge of sarcasm here. Nobody should be this afraid to give their name to someone in order to get a sandwich. But you touch upon a good point, regardless of whether or not it was intentional. Lying is perfectly acceptable in such situations. People give out way too much personal information to other people who not only don't require it but who have no way on earth of verifying it in the first place. The same holds true for the many entities that ask for your Social Security Number. Unless they are the government, a financial institution, or someone who is planning on running a credit check, any number will do as it is only used for verification the next time you speak to them. We don't mean to buy into the pervasive paranoia that insists on suspicion of all those around us and thinks of trust as a four letter word. But at the same time, people need to know they are free to be anyone they wish in a sandwich shop or elsewhere.

Dear *2600*:

Last night my girlfriend and I were at a local Meijer super store. Most times I'll just go to the register to check out. The employees are usually friendly enough. We were in a bit of a hurry this time, so we went to the U-Scan. I had some cash on me and she had her debit. I *assumed* that because after I put in my cash and the "other payments" option was still on the screen that the programmers of the U-Scan were bright enough to figure out that if a card is swiped to only charge the difference. No dice. Instead, the machine *flips out!* The under-trained employee didn't ask us what happened. He just simply canceled the order and printed a receipt. Apparently the machine didn't even record that I put money into it. Or, if it did, he deleted it. Regardless, all he did to do this was touch the corner of the screen, type 27, then type 240. I'm assuming one of the numbers is a store number and the other is his employee ID. The menu was *very* simple; a monkey could navigate through it. With a bit of a distraction it seems like you could start printing your own receipts! This is stealing and illegal so don't! But it's always fun to play with Meijer employees.

chemdream

Dear *2600*:

Greetings all. Further to my letter in the last issue, I thought that you'd be interested in hearing about this. Tesco (and, to my knowledge, ASDA too) have just installed a spate of "self-service checkouts." This is quite a new thing for the U.K. The supplier is NCR, and the model is their "FastLane" system (http://www.➥ncr.com/en/products/hardware/sa_selfchk.htm). I haven't had a chance to try the usual "tap the four corners" and other methods to get to setup screens. I'm sure that others have, but I have always been too busy whilst using one to have a chance to. I have noticed this, however. When you choose to pay with a credit/debit card, the system will scan your card but won't ask for a PIN number nor a signature. You swipe your card and it will just sit there and store the number and charge your account (just like the other till (POS) systems do). This is quite worrying, as I'm sure you are already aware, from a (in)security point of view. It isn't a difficult colligation to say that "this is the most laxly secured idiocy ever to help fraudsters." I wonder what else these esteemed developers will decide to thrust upon the unsuspecting sheep-flock of a public that we have.

Keep your cards close and their details closer.

Marxc2001

Dear *2600*:

Last year I decided that a regular cell phone service plan wasn't for me anymore. I went to Radio Schlock and bought a Cingular phone and a prepaid card with cash. Because I could, I provided all bogus info for this phone (name, home address, home phone, and Social Security Number). I declined the request for a photo ID and I walked out with a working phone.

After a few weeks I realized that certain people couldn't call me. From most telephones there was no problem but many phones from inside and outside the Cingular network would get a "this number is disconnected" message. I knew that something in Cingular's routing was messed up, probably from someone previously having this number and then it being disconnected. I called tech support.

After four hours on the phone over three days (not including hold time), Cingular attempted various high-tech fixes to my problem. The tech would bang on their keyboard and then say, "Have your friend try to call you now. Did it work? No? OK. Hold on." Repeat ad nauseam. It was clear they really didn't know what they were doing even as my call was escalated higher and higher.

Finally the rep at the "highest" level of escalation told me, "I'm going to try one more thing and if it doesn't work, we'll have to issue you a new SIM card and new phone number." This was a bogus alternative. Why not *fix* the problem instead of waiting for this number to be reassigned to someone new where the problem could repeat itself? Anyway, against all odds, Cingular's "last chance" fix worked. "Great!" I thought. Problem solved. In fact, as I would discover a few hours later, it was "super-solved."

When using a prepaid plan the cell phone receives a text message after each call with the cost of the previous call and the current balance. The messages

are a little annoying but, like everything else, eventually you learn to ignore them. It took me a whole afternoon of calls to realize I wasn't getting these messages anymore. Curious, I pinged the network with #777 to request my account balance. Then I made a few calls to some friends at their land line. I pinged the network again and the balance was the same. Hurrah!

In their desperate and haphazard effort to fix my phone they disconnected it from their billing system! My prepaid phone was now a free phone! Also, Cingular had no idea who I was. The worst they could do was deactivate my phone. They had no one to send a bill to. Needless to say, I felt more than compensated for my hours on hold.

I enjoyed this perk for nine months before the phone turned on one morning to show "SIM card registration failed." I called tech support again and after several escalations and "it shouldn't do this" quotes from the reps, my phone was reactivated, albeit with a $0.01 balance. I'm paying for phone service again but I will fondly remember my months with a free phone.

This was an interesting experience and it shows that proper phone operation is a separate entity from billing. You can have one without the other. I hope this is interesting to people who are curious about how the phone service works.

Zaphod_B

Dear *2600*:

Thought you might appreciate the fact that not only is *2600* not hidden at the back of the shelf in the Charlottesville, Virginia Barnes and Noble, but it's also front and center, eye level, and a "featured title."

ben

There are many such stores all over the place where we're proudly displayed. We tend to hear more about the exceptions so it's important to acknowledge when stores do a good job, as most of them do.

Provocation

Dear *2600*:

I had just purchased your magazine from a very attractive female type unit while talking on the phone about a comic con. I was putting it into my inside jacket pocket when I too was assaulted by your wonderfully smelling pages. This resulted in me sucking my thumb. I think my chances of hitting it off with her are now less than zero. I thought there were gonna be warnings about this sort of thing. At any rate keep up the great work. Love the smell of a fresh baked issue.

Tapi

Dear *2600*:

So I was at the #2600 IRC channel chatting about the Microsoft and Novell partnership asking people what they thought about this. Anyhow, to make a long story short I was spelling Microsoft like this: micro$oft. I got kicked from the channel for using bad language (three times resulted in a ban). So my question is, when did micro$oft become a bad word on the #2600 channel?

ghOstb0t

We are in no way responsible for any such random actions that occur in our IRC channel. We suspect you were the victim of someone's opinion/joke, not to mention your failure to realize that repeatedly doing the same thing would get you banned. We encourage readers to check out the #2600 channel (and other regional 2600 channels) on the irc.2600.net network. Just remember that we don't control the intelligence level. While people from the magazine try to come onto the channel from time to time, it's mostly a wide open space where users from all levels of the human evolutionary scale congregate. Keep this in mind and you won't get overly frustrated.

Appreciation

Dear *2600*:

First, I need to thank you. I have thoroughly enjoyed your magazine for a few years now. I've learned a ton and it's been very useful in conveying the mentality that so many of us share to the outside world. Many times I've answered questions by simply presenting your magazine to the curiosity seekers.

Second, I was 17 when the FBI first raided my home. I was 19 the second time around. I was 21 when I was sentenced in 2005 to 17.5 years in federal prison. And because of my charges and what I had admitted to doing and what I was told to expect, that sentence was quite a shock. No, not pedophilia or even sex-related. Not drug-related. A minor role in a credit card fraud scheme. The judge apparently was none too happy with me, giving me the statutory maximum.

I would love to write an article for you describing what exactly it's like to go from bad to worse to worst. A report from the front lines, if you will. My hope is that in the "unlikely" event that any *2600* readers are ever charged by the feds, they won't receive five to six times the sentence they expect, as did I. I would most like to spread the word about how dirty feds can, and will, play. And a few points to watch out for.

Let me know if you might like me to write you a little article. And thanks again guys.

Jason C.

By all means write the article. Your story serves as a reminder to those who may not yet know it that the prosecution will do anything - including lying to you - in order to secure a conviction. Putting people away is their business. While there are many overly expensive, incompetent, and dishonest lawyers out there, you are still far better off getting one rather than trying to work things out with the authorities on your own. We've heard so many horror stories of people getting screwed at sentencing and with today's prosecutorial climate, it's bound to get even worse. And, needless to say, this sort of thing does nothing for rehabilitation.

Continued from page 19

```
        lrnd = ltable(lrnd);                    /* get the next lookup table value */
        ilen = (U)(lrnd / 832 + 256);           /* buffer bitlen: 256<=ilen<=1516 */
        if (ibit + ilen > ibuf * 8) {           /* curr. bit-pointer+ilen spans cbuf */
           if (ieof) {                                        /* EOF flag is ON */
              ilen = ibuf * 8 - ibit; /* reset bit-length of buffer segment */
           } else {                   /* EOF flag is OFF; adjust file pointer */
              ifn_write(cbuf, lbyt, ibuf, ebuf);  /* write data to the file */
              lbyt -= (ibuf - ibit / 8);       /* set lbyt to load from ibit */
              ibit %= 8;               /* set ibit to first byte of <new> cbuf */
              break;                     /* exit loop to reload cbuf from lbyt */
           }
        }                     /* encrypt or decrypt the current segment [below] */
        for (indx = 0; indx < ilen; indx++) { /* loop through array elements */
           int1[indx] = indx;           /* bit offsets from current ibit offset */
           lrnd = ltable(lrnd);            /* get the next lookup table value */
           lnt2[indx] = lrnd;              /* lookup values for sort function */
        }
        ifn_sort(int1, lnt2, istk, ilen - 1);            /* sort lookup array */
        memcpy(ctmp, cbuf, 2048);          /* copy data buffer to dest. buffer */
        if (iopr) {                              /* this is the encrypt operation */
           for (indx = 0; indx < ilen; indx++) {   /* loop through bit group */
              bitput(ctmp, indx + ibit, bitget(cbuf, int1[indx] + ibit));
           }                           /* move bits to "random" positions [above] */
        } else {                                /* this is the decrypt operation */
           for (indx = 0; indx < ilen; indx++) {   /* loop through bit group */
              bitput(ctmp, int1[indx] + ibit, bitget(cbuf, indx + ibit));
           }                    /* restore bits from "random" positions [above] */
        }
        memcpy(cbuf, ctmp, 2048);          /* copy dest. buffer to data buffer */
        ibit += ilen;                     /* increment ibit to next bit-segment */
        if (ibit == ibuf * 8) {            /* loop until ibit == length of cbuf */
           ifn_write(cbuf, lbyt, ibuf, ebuf); /* put current buffer to file */
           ibit = 0;                      /* set ibit to first byte of <new> cbuf */
           break;                         /* ibit == length of cbuf; exit loop */
        }
     }
  }
  free(cbuf);                                  /* deallocate the file buffer */
  free(ctmp);                                  /* deallocate the temp buffer */
  free(int1);                               /* deallocate the sort index array */
  free(lnt2);                              /* deallocate the sort lookup array */
  free(istk);                               /* deallocate the sort stack array */
}

I bitget(C *cstr1, I ibit) {                    /* get a bit-value from a string */
  I ival;                                        /* initialize the bit value */

  switch (ibit % 8) {                        /* switch on bit# within character */
     case 0:                                    /* bit #0 in target character */
        ival = 1;                                          /* value of bit #0 */
        break;
     case 1:                                    /* bit #1 in target character */
        ival = 2;                                          /* value of bit #1 */
        break;
     case 2:                                    /* bit #2 in target character */
        ival = 4;                                          /* value of bit #2 */
        break;
     case 3:                                    /* bit #3 in target character */
        ival = 8;                                          /* value of bit #3 */
        break;
     case 4:                                    /* bit #4 in target character */
        ival = 16;                                         /* value of bit #4 */
        break;
     case 5:                                    /* bit #5 in target character */
        ival = 32;                                         /* value of bit #5 */
        break;
     case 6:                                    /* bit #6 in target character */
        ival = 64;                                         /* value of bit #6 */
        break;
     case 7:                                    /* bit #7 in target character */
        ival = 128;                                        /* value of bit #7 */
        break;
     default:
```

```
      break;
   }
   return ((cstr1[ibit / 8] & ival) != 0);
}                          /* return the value of the target bit [above] */

V bitput(C *cstr1, I ibit, I iput) {          /* put a bit-value to a string */
   I ival;                                     /* initialize the bit value */
   I ipos = ibit / 8;                     /* position of 8-bit char. in cstr1 */

   switch (ibit % 8) {                     /* switch on bit# within character */
      case 0:                                 /* bit #0 in target character */
         ival = 1;                                     /* value of bit #0 */
         break;
      case 1:                                 /* bit #1 in target character */
         ival = 2;                                     /* value of bit #1 */
         break;
      case 2:                                 /* bit #2 in target character */
         ival = 4;                                     /* value of bit #2 */
         break;
      case 3:                                 /* bit #3 in target character */
         ival = 8;                                     /* value of bit #3 */
         break;
      case 4:                                 /* bit #4 in target character */
         ival = 16;                                    /* value of bit #4 */
         break;
      case 5:                                 /* bit #5 in target character */
         ival = 32;                                    /* value of bit #5 */
         break;
      case 6:                                 /* bit #6 in target character */
         ival = 64;                                    /* value of bit #6 */
         break;
      case 7:                                 /* bit #7 in target character */
         ival = 128;                                   /* value of bit #7 */
         break;
      default:
         break;
   }
   if (iput) {                                        /* OK to set the bit ON */
      if (!(cstr1[ipos] & ival)) {                   /* bit is NOT already ON */
         cstr1[ipos] += ival;                  /* set bit ON by adding ival */
      }
   } else {                                          /* OK to set the bit OFF */
      if (cstr1[ipos] & ival) {                     /* bit is NOT already OFF */
         cstr1[ipos] -= ival;                  /* set bit OFF by subt. ival */
      }
   }
}

V ifn_sort(I *int1, L *lnt2, I *istk, I imax) {   /* array Quicksort function */
   I iex1;                              /* initialize the outer-loop exit flag */
   I iex2;                              /* initialize the inner-loop exit flag */
   I ilap;                                 /* initialize the low array pointer */
   I ilsp;                                 /* initialize the low stack pointer */
   I irdx = 0;                                   /* initialize the sort radix */
   I itap;                                 /* initialize the top array pointer */
   I itsp;                                 /* initialize the top stack pointer */
   I ival;                  /* initialize array value from low stack pointer */
   L lva2;                  /* initialize array value from low stack pointer */

   istk[0] = 0;                            /* initialize the low array pointer */
   istk[1] = imax;                         /* initialize the top array pointer */
   while (irdx >= 0) {                           /* loop until sort radix < 0 */
      ilsp = istk[irdx + irdx];                 /* set the low stack pointer */
      itsp = istk[irdx + irdx + 1];             /* set the top stack pointer */
      irdx--;                                    /* decrement the sort radix */
      ival = int1[ilsp];           /* get array value from low stack pointer */
      lva2 = lnt2[ilsp];           /* get array value from low stack pointer */
      ilap = ilsp;                              /* set the low array pointer */
      itap = itsp + 1;                          /* set the top array pointer */
      iex1 = 0;                       /* initialize the outer-loop exit flag */
      while (!iex1) {                  /* loop to sort within the radix limit */
         itap--;                          /* decrement the top array pointer */
         if (itap == ilap) {           /* top array pointer==low array pointer */
            iex1 = 1;                     /* set the outer-loop exit flag ON */
```

```
        } else if (lva2 > lnt2[itap]) {   /* value @low ptr > value @top ptr */
           int1[ilap] = int1[itap];        /* swap low and top array values */
           lnt2[ilap] = lnt2[itap];        /* swap low and top array values */
           iex2 = 0;                    /* initialize the inner-loop exit flag */
           while (!iex2) {             /* loop to compare and swap array values */
              ilap++;                     /* increment the low array pointer */
              if (itap == ilap) {     /* top array pointer==low array pointer */
                 iex1 = 1;                /* set the outer-loop exit flag ON */
                 iex2 = 1;                /* set the inner-loop exit flag ON */
              } else if (lva2 < lnt2[ilap]) { /* value@low ptr<value@low ptr */
                 int1[itap] = int1[ilap];  /* swap top and low array values */
                 lnt2[itap] = lnt2[ilap];  /* swap top and low array values */
                 iex2 = 1;                /* set the inner-loop exit flag ON */
              }
           }
        }
     }
     int1[ilap] = iva1;            /* put array value from low stack pointer */
     lnt2[ilap] = lva2;            /* put array value from low stack pointer */
     if (itsp - ilap > 1) {                          /* low segment-width is > 1 */
        irdx++;                                     /* increment the sort radix */
        istk[irdx + irdx] = ilap + 1;                /* reset low array pointer */
        istk[irdx + irdx + 1] = itsp;                /* reset top array pointer */
     }
     if (itap - ilsp > 1) {                          /* top segment-width is > 1 */
        irdx++;                                     /* increment the sort radix */
        istk[irdx + irdx] = ilsp;                    /* reset low array pointer */
        istk[irdx + irdx + 1] = itap - 1;            /* reset top array pointer */
     }
  }
}

V ifn_msgs(C *cmsg, I iofs, I irow, I icol, I ibrp, I iext) { /* display msgs */
  if (iofs >= 0) {                                        /* OK to clear screen */
     io_vcls(7);                                           /* clear the screen */
  }

  io_vdsp(cmsg, 4, abs(iofs), 7);                      /* display the user message */
  if (ibrp) {                                    /* OK to sound user-alert (beep) */
     printf("\ a");                                      /* sound the user-alert */
  }
  if (iext) {                                          /* OK to exit the program */
     io_vcsr(5, 0, 0);                                  /* relocate the cursor */
     fcloseall();                                      /* close all open files */
     exit(0);                                                /* return to DOS */
  } else {                                            /* do NOT exit the program */
     io_vcsr(irow, icol, 0);                              /* 'hide' the cursor */
  }
}

L ltable(L lrnd) {                                     /* get next lookup table no.*/
  L l1;                                               /* initialize temp value #1 */
  L l2;                                               /* initialize temp value #2 */
  L l3;                                               /* initialize temp value #3 */
  L l4;                                               /* initialize temp value #4 */

  l1 = lrnd % 8;                           /* These 5 lines are an integer-only */
  l2 = (lrnd - l1) % 16;                    /* equivalent to the floating-point */
  l3 = (lrnd - l1 - l2) % 64;              /* operations formerly used in this, */
  l4 = (lrnd - l1 - l2 - l3);             /* the 16-bit DOS version of the code */
  return (l1 * 214013 + l2 * 82941 + l3 * 17405 + l4 * 1021 + 2531011) % 1048576;
}

V ifn_read(C *cbuf, L lbyt, U ibuf, FILE *ebuf) {     /* read from binary file */
   fseek(ebuf, lbyt, SEEK_SET);                    /* set the buffer-read pointer */
   fread((V *)cbuf, 1, ibuf, ebuf);             /* read data from the binary file */
}

V ifn_write(C *cbuf, L lbyt, U ibuf, FILE *ebuf) {    /* write to binary file */
   fseek(ebuf, lbyt, SEEK_SET);                     /* set the buffer-write pointer */
   fwrite((V *)cbuf, 1, ibuf, ebuf);             /* write data to the binary file */
}

U io_vadr(I inop) {                              /* get video address (color or b/w) */
```

```
   rg.h.ah = 15;                                  /* video-address function */
   int86(0x10, &rg, &rg);                        /* call DOS for video address */
   if (rg.h.al == 7) {                                  /* register A-low is 7 */
      return(0xb000);                                   /* return b/w address */
   } else {                                           /* register A-low is NOT 7 */
      return(0xb800);                                   /* return color address */
   }
}

V io_vcls(I iclr) {                                     /* clear screen function */
   I irow;                                  /* initialize the row number variable */
   C cdat[81];                               /* initialize the row data buffer */

   memset(cdat, ' ', 80);                              /* clear the row data buffer */
   cdat[80] = '\0';                                 /* terminate the row data buffer */
   for (irow = 0; irow < 25; irow++) {                  /* loop thru the screen rows */
      io_vdsp(cdat, irow, 0, iclr);              /* display each <blank> screen row */
   }
}

V io_vcsr(I irow, I icol, I icsr) {              /* set cursor position [and size] */
   rg.h.ah = 2;                                        /* cursor-position function */
   rg.h.bh = 0;                                              /* video page zero */
   rg.h.dh = (C)irow;                                           /* row number */
   rg.h.dl = (C)icol;                                        /* column number */
   int86(0x10, &rg, &rg);                          /* call DOS to position cursor */
   if (icsr) {                                          /* cursor-size specified */
      rg.h.ah = 1;                                      /* cursor-size function */
      rg.h.ch = (C)(13 - icsr);                        /* set cursor-begin line */
      rg.h.cl = 12;                                      /* set cursor-end line */
      int86(0x10, &rg, &rg);                        /* call DOS to set cursor size */
   }
}

V io_vdsp(C *cdat, I irow, I icol, I iclr) {            /* display data on screen */
   I ilen = strlen(cdat);                        /* length of string to be displayed */
   I iptr;                                      /* byte-counter for displayed string */
   U uclr = iclr * 256;                        /* unsigned attribute high-byte value */

   if (!uvadr) {                                    /* video pointer segment not set */
      FP_SEG(uvadr) = io_vadr(0);                      /* set video pointer segment */
   }
   FP_OFF(uvadr) = irow * 160 + icol * 2;              /* set video pointer offset */
   for (iptr = 0; iptr < ilen; iptr ++) {             /* loop thru displayed string */
      *uvadr = uclr + (UC)cdat[iptr];                  /* put data to video memory */
      uvadr++;                                    /* increment video display pointer */
   }
}
```

Techno-Exegesis

by Joseph Battaglia
sephail@2600.com

...or maybe not. Maybe new technology isn't such a good thing. Perhaps we've reached a point where the desire to incorporate it into every aspect of our lives has begun to take precedence over the goal of what it is we're trying to replace. It's not like there's been any lack of concern over the matter, especially lately. Search any news aggregating service for the terms *+voting +machine +fraud* and you'll see what I'm talking about. What about *+passport +cracked* or *"red light" +camera*? I'm not referring to dried-out passports whose covers have succumbed to old age, or the little LED that indicates your latest burglary attempts have been captured on two slowly rotating reels of magnetic tape (although these are surely problems to some). I'm talking about the excessive use of technology. Five years ago there was no such thing as intercepting the communications between an immigration control computer and your passport, and ten years ago you weren't likely to get an automated ticket in the mail because you entered an intersection behind that Big-Ass SUV which entirely blocked your view of the traffic light as it changed from green to red. And it's not like this stuff is helping anything.

The RFID "feature" of a passport is, as far as I'm concerned, entirely useless. It creates an unnecessary security risk and contributes nothing to the speed at which immigration lines progress. The current system uses MICR (magnetic ink character recognition) as the agent swipes the bottom portion of your passport. It's fast, relatively reliable, perfectly suitable for the application, and it's even secure (so long as the passport remains in your possession). But we're rapidly progressing to the point where anyone can sneak up behind you with a specially designed RFID reader stuffed in their crotch, brush up against your tuckus, and suck the digital fingerprints and photographs of you and your kids straight out of your ass-pocket. No shit. And every time this stuff is demonstrated, officials shrug it off as overly paranoid. They don't understand the technology, yet are responsible for making all of the decisions regarding its use.

What about the red light cameras? Surely some entity besides the capitalizing municipality and associated police officers (who have dutifully acquired extended donut breaks as a result of the reduced workload) stands to benefit from them. They've got to be making our streets safer, since that's the only *official* reason generally given for their existence. But even this is disputed, as the *Washington Post* has discovered upon investigation of red light cameras installed in D.C. In fact, accidents have more than doubled in some locations and there are even lawsuits claiming that municipalities have changed light timings to increase violations! What is clear is that accidents are increasing in many locations (and that there's about $100 missing from my checking account). A simple solution comes to mind: remove the damn cameras and just delay the perpendicular green light by a few seconds. The T-bone crashes that they're looking to prevent would surely be reduced without the added side-effect of increased rear-end collisions. It's unfortunate that such a choice between safety and income never leans in our favor.

The grandmaster of all failing technological implementations these days seems to be the voting machine. Ah, the voting machine. Few of us can even remember when the activities of voting and using a machine were two entirely separate processes. Voting *used to* entail marking your favorite candidates onto a sheet of paper to have it later counted by the King's Men, who could not be trusted. Now the vote counters have been replaced with elaborate mechanical and electrical contraptions, which

cannot be trusted. Corrupt poll workers, loose gears, broken levers, and even hanging chads were no match for the commotion stirred up by the poor design of the modern electronic voting machine. The documentary *Hacking Democracy* conveys this very well; you've got to watch it. Not only does it demonstrate how access to the most widely-handled component of these machines can be used to skew elections, but it even sheds some doubt as to whether or not the public willingly elected some of the lesser-evolved members of our species into some of the most critical positions in our social hierarchy. Not that I'm a conspiracy theorist or anything....

Not everybody is so eager to replace everything with the latest and greatest gadgets, however. Take pilots, for instance. When planning flights, many pilots use an E6B (or similar) flight computer. It's a computer in the most rudimentary sense of the term, essentially a special-purpose slide rule. In fact, it's the only field in which slide rules are still in widespread use. Why? Because they're fast, reliable, and when you're thousands of feet above the ground flying an aircraft you don't care to be fumbling with an electronic calculator: replacing dead batteries, trying to work around that stuck key, or wondering whether or not the LCD would still be intact after sitting on it, if only you'd started that diet a few months earlier. There are other added benefits, too. The concepts of significant digits and keeping track of exponents are generally lost amongst today's TI-89-touting youth. Slide rules require that you consider these things, often allowing you to catch mistakes long before you would while using a calculator.

Look, I'm not anti-technology. Really. I practically immerse my entire life in it. It just seems obvious that some things aren't quite ready for prime time yet, and premature deployment may actually have the potential for some devastating consequences. The examples I used here are simply those that have either received a bunch of press coverage or that I have personal experience with. I threw in the slide rule rant for good measure (no pun intended), but the concepts they demonstrate are well-suited to the notion that there are some scenarios where old technology just works better. There are plenty more I could have chosen along the same lines, some with more severe ramifications and some which are much more trivial. Either way, it usually seems to be the younger generation who are just as closed-minded to using more traditional technology as your grandmother is toward the advent of e-mail. Whether it's ending up with a corrupt democracy, rampant identity theft, higher accident rates, or a broken calculator when you need that quick altitude-correction calculation, we definitely need to take a good hard look at the benefits and drawbacks of making the switch to the latest-and-greatest.

GasJack - Hijacking Free Gasoline

by cipz
cipz@lv2600.com

Giant is a food store chain and some stores have gas stations. It actually has a long and complicated history, none of which pertains to this hack. Like many large food stores, they have a program which offers their shoppers rewards for using their BonusCard at every purchase. Shoppers accumulate points which are traded in for discounts. All the caveats of having your personal shopping habits tracked apply but have nothing to do with this article.

There are several different types of points a shopper can collect. The ExtraRewards points allow shoppers to get up to a 15 percent discount on their next shopping bill. It is the new GasRewards points that has peaked my curiosity. For every one hundred dollars a shopper spends, they receive a discount of ten cents off a gallon at the gas pump. According to Giant's own policy for this promotion, gas can be obtained for free if enough points are earned. The policy however dictates that the points can only be redeemed once and the discount only applies up to 30 gallons. This means you get one fill of your gas tank at the earned discount. It has not been confirmed, but a friend mentioned having a vehicle which holds about 32 gallons of gas that was filled at the discounted price. It appears the 30 gallon limit might not be enforced. There also does not exist any policies on gas cans. A scenario: John accumulates 500 gas points and decides to cash in his points because the deadline for the promotion is fast approaching. He proceeds to the gas pump, swipes his BonusCard under the bar code reader and, voila, gas now flows at a rate of 50 cents less a gallon. His tank holds 30 gallons and he manages to save himself 15 dollars.

First Mistake

The Giant BonusCard is nothing more than a piece of plastic with a UPCA barcode. The Giant BonusCard number (BCN) is 11 digits while the 12th digit, a checksum, is omitted. The BCN is printed at the top of every receipt. That was Giant's first mistake. A simple solution is to adopt the practice of credit card receipt printers: only print the last four digits of a card. Unfortunately, there are more mistakes and holes which make instituting this single change ineffective at stopping account hijacking.

Game Over

This article would be over if the goal was as simple as obtaining gas for free. A person of questionable ethical fortitude could easily find Giant receipts in the garbage and then proceed to one of many online references to have the BCN converted to a printable barcode. Then just swipe the barcode at the gas pump and drive off with discounted gas. But if one objects to putting their hands in places of questionable sanitary fortitude, there exists another method. Randomly generating bar codes and then using the in store scanners to see if the accounts exist and how many gas points are on them is one idea. Again, this article would be over quickly leaving the reader the daunting task of trying to figure out which numbers were valid and which accounts had enough points to make a trip to the pump worth the effort.

Internet to the Rescue

Whenever I have to do something that is boring and repetitious, the first thing I think of is how I can get a computer to do it for me. Even if the original task were to take only 10 minutes, I would gladly spend an hour writing a program to make the computer do it for me in 10 seconds because, some day, I might have to repeat the task. I hear some blah blah blah about efficiency, but to me programming is fun! The goal now was to find a website which allowed shoppers to check the balance of their Giant BonusCards. I located several websites which all appear to be official Giant websites.

Trying to Save Time by Wasting 15 Minutes

One of particular interest was the site www.giantfood.com/bonuscard/. At first glance I was surprised to see that the first three letters of the shopper's last name were required and even more surprised that this system was requiring 12 digits instead of 11 to log in. I headed over to the U.S. Census Bureau and downloaded a file which listed the most common surnames in the United States and the number of people per surname. Using a simple script to chop the first three characters off, add up the population numbers, and resort the list, I compiled my own new list. The original list contained over 16,000 entries. The new list contained less than 3000 entries. Using pure brute forcing, guessing a three character word has 17,576 (26^3) possibilities. Rather than throw my new list at the site and allow it to brute force the last name, I decided to try and log in using a known

valid set of credentials. After several attempts with valid information I concluded the log in function of this site was not working. I just wasted 15 minutes, but oh well, I got a dictionary of common surnames in the U.S. I am sure that might come in handy one day. And in case anyone was wondering, yes, Smith was the most common.

I'm In!

www.giantpa.com was another site which looked promising. Unfortunately it asked for a username (email), password, and BCN to log in. I entered a known valid BCN and spoofed the rest of the information. I ran Ethereal (packet sniffer) and Achilles (proxy) and logged the data because I was sure it would be useful later on. My jaw dropped as I was taken to a page which listed the first name and the savings so far this year of the BCN owner. I noticed a link to check on the various promotion points and followed it. True to the link's promise, I was presented with the amount of points of the several promotions which the BCN owner was eligible for. Among them was the amount of GasRewards points. Two more huge mistakes on Giant's part was allowing default logins and submitting data in plain text.

More Than Just Free Gas

Again, this article would end here for anyone wishing to hijack free gasoline. A person with adequate programming capabilities and dubious intentions could write a program to simply step through BCNs and log the amount of points each one has at the time. Then it is just a matter of printing off the barcode and heading out to the gas station. As I was writing a program to test this theory, I noticed there were some differences between the information presented when I logged in. Some BCNs would first ask for me to select a preferred store but would always come back with a generic first name, like John, Betty, Pat, Mary, etc. and would always have $0.00 savings this year. I assumed these BCNs to be invalid or not ever registered. Another response I was getting was a failed login attempt. I chose not to investigate this any further. The most interesting response I received was the rare ability to click a link which read "Update Account." Following this link presented me with a wealth of information. The information gathered from this new link included a password (keep in mind, the password to get this far was originally dummy information). The password was in a form which made it appear as masked characters, but viewing the source or the ethereal logs showed the password coming across the wire in plain text. Huge Mistake Number... a lot... Never send users' their passwords, ever. Instead, make them confirm the old password first if they want to change it, or implement a password reset policy which emails the user their password. Analyzing the html of the different responses also kicked up a hidden piece of information: the preferred store number of the owner of the BCN. Using the Store Locator page, one easily matches store numbers to store addresses. I believe the creators of the BonusCard program were thinking "Who would ever *want* to hack this?" which led to the complete lack of security I have seen. Anyone designing any online system should build in security from day one, especially if you collect even a single piece of information from your users. umount /dev/soapbox

The Gory Details

Please keep in mind, I am by no means an expert on http or programming. I taught myself what I needed to know in order to get the programs to work. When one visits the website, a JSESSIONID is created in a cookie. Then the login credentials along with the JSESSIONID are sent to the server using a POST method. The server then establishes a session using the JSESSIONID. This JSESSIONID is not checked against the IP address of the client and can be arbitrarily specified by the client. To make things easier during development, I simply used the BCN as the JSESSIONID. The server then sends back a 302 Moved Temporarily message. The location field in this message is a full URL which contains more tokens and the previously mentioned JSESSIONID. This link can be followed by anyone, which opens up the possibility of session hijacking. This 302 location is retrieved using a GET request and must be followed in order to initialize the session. If an attempt is made to request the points page after sending the POST data, the server will respond with an error stating the storenum variable has not been defined. Requests for the pages containing the points information are made using GET /shareddev/subclub/. All the points the customer has for the reward clubs the BCN is eligible for are displayed.

The Code

The code is written in Ruby because I wanted to learn more about Ruby. It is easily portable to Perl, but I will leave that as an exercise to the reader. The betweenstrings() function could probably be simplified using regex, but this function has served me well in the past and I am still learning regex. No error checking was built in to this code as it was designed to be a proof of concept. The POST and GET strings have been stripped to a minimum so no browser cloaking is done. If you put a for loop around this code and giantpa.com's thugs kick in your door, do not come crying to me. It only works for an account which is eligible for Gas Reward points and will return an error if the store locator or failed login situations occur. Code is not needed for this hack, but it does help explain the underlying system, expose its vulnerabilities, and simplify the overall demonstration.

The Risks

I identified several risks throughout working on this project. First, dumpster diving has all of its risks of being caught associated with it. This may not be a risk, but more of an ethical choice to make. Following through on this method essentially steals the points earned by someone else. During the initial course of probing the website, I caused errors to be generated. These errors reported my IP address. Tagging the

server with several thousand requests to login may disturb the sleeping IT security guard. After printing off a bar code to try, there are risks associated with actual procurement of the free gas. These gas stations typically have a booth where a person sits to collect cash. Most of the time I see this person reading a book and suspect exiting the booth is not permitted. Almost any gas station will employ the use of security cameras, but again, this risk is minimized by the response time to the incident. Retention time of the video is likely to be short while the chain of events leading to request to view the videos will take longer. First, the shopper whose BCN was hijacked must complain when they notice the problem. This may be shortly after paying for the gas at full price. It is very difficult to motivate a company which has already been paid. So the shopper complains to the attendant. The attendant hails a shift manager. The shift manager is perplexed and hails a store manager. At this point, the complaining customer will have probably been appeased. Assuming an isolated incident, it is likely the investigation will stop here. Otherwise, it is probably up to the store manager to make the connection that accounts are being hijacked. I am pretty sure that getting caught is legally binding (all sorts of puns intended on that one).

Does It Work?

After identifying a lot of the risks, I decided to test the method using my own BCN. I simply ran my BCN through my program, determined the amount of discount, printed the bar code, and headed out to the gas station. I was rewarded with the discount I was entitled to while retaining the ability to sleep peacefully at night.

Further Investigations

I did not go after the underlying database of the BonusCard system. I am sure with the lack of security observed, the site is vulnerable to database query injection and XSS attacks. The server is running Cold Fusion and one error message I received was nondescript. I googled it and turned up information about Cold Fusion running on IIS. Again, none of this was relevant to the project, so the details may be fuzzy. I did not loop through massive amounts of BCNs to determine different account types. I merely sampled a few participating friends' BCNs and may have accidentally mistyped a few which lead to the identification of the different account types. Failed logins were not investigated as to why they failed, just that they were consistently coming up as failed. Store locator logins were also not further investigated. Updateable accounts were extremely rare, and any found were the same. I suspect these were test accounts. The database contained the first name of the BCN owner and it is reasonable to assume it contains all the information on the BonusCard application form. I am very much still interested in the Giant BonusCard system and all the fun it can provide.

Shouts to milkman for his ruby help and to LV2600.com for putting up with me.

```
GasJack.rb
require 'socket'

def betweenstrings(searchtext,startstring,endstring,startindex)
  searchtextlength = searchtext.length
  startstringlength = startstring.length
  endstringlength = endstring.length
  if searchtextlength == 0 or startstringlength == 0 or endstringlength == 0
    return ""
  else
    if searchtextlength - (startstringlength + endstringlength) <= 0
      return ""
    else
      startstringindex = searchtext.index(startstring,startindex)
      if startstringindex == nil then
        return ""
      else
        endstringindex = searchtext.index(endstring,startstringindex + startstringlength)
        if endstringindex == nil
          return ""
        else
          betweenstringslength = endstringindex - (startstringindex + startstringlength)
          return searchtext[startstringindex + startstringlength,betweenstringslength]
        end
      end
    end
  end
end

puts "Enter 11 digit BonusCard number"
bcn = gets
sck = TCPSocket.new('www.giantpa.com', 'www')
post_string = "POST /shareddev/Giant_register/login_action.html HTTP/1.1\ nContent-Type:
application/x-www-form-urlencoded\ nHost: www.giantpa.com\
```

```
nContent-Length: 63\ nCookie: JSESSIONID="+bcn+"\ n\ n"+"F_
Username=a&F_Password=a&F_BonusCard="+bcn+"&Login=Sign+In\ n"
sck.print post_string
answer_post = sck.gets(nil)
sck.close

location302 = betweenstrings(answer_post,"location: http://www.giantpa.com","\ n",0)
location302.chop!
get302_string = "GET "+location302+" HTTP/1.1\ nHost: www.
giantpa.com\ nCookie: JSESSIONID="+bcn+"\ n\ n"

sck = TCPSocket.new('www.giantpa.com', 'www')
sck.print get302_string
answer_get302 = sck.gets(nil)
sck.close

sck = TCPSocket.new('www.giantpa.com', 'www')
getpoints_string = "GET /shareddev/subclub/ HTTP/1.1\ nHost: www.
giantpa.com\ nCookie: JSESSIONID="+bcn+"\ n\ n"
sck.print getpoints_string
answer_getpoints = sck.gets(nil)
sck.close

gaspoints = answer_getpoints[/You have \ d* Gas Extra Rewards points/]
gaspoints = betweenstrings(gaspoints,"You have "," Gas Extra Rewards points",0)
puts gaspoints
```

Motorola IMfree as a Wireless iTunes Remote

by Kcahon

About a year ago Motorola put out a product called the IMfree. It was a wireless instant messenger that connected to a base station on a regular PC. The station communicated with the device over radio frequencies, which gave it a range of about 50 yards. At the time it looked like a good buy and I purchased it for $100. I quickly realized that I had little use for it, as I had access to a machine with AIM on it anyway. Many people must have felt the same way and the price plummeted to around $30. It sat around for awhile until I had an epiphany. Wouldn't this make a perfect iTunes remote?

Several people were already hacking it and I found some message boards that were dedicated to its development. One such forum, http://teknikill.➥net/bbs/, was especially enlightening. This site had appeared on Hackaday.com and I would occasionally check in to see what was going on. There awaited me the thread "imfree and winamp" which had been posted by a user named Jason. In there it described an ingenious way of having the IMfree communicate with Winamp. The "event" feature in Trillian Pro (a popular IM client) enables a program or action to be executed from any screen name remotely with just a plaintext message. This set off fireworks in my mind.

The next day I opened up iTunes and it hit me. Millions of people use iTunes and rely on it for music. Would I be able to integrate the IMfree with iTunes so that it could play a song, skip to the next song, and do a whole universe of functions? All wirelessly? It was within my grasp. The following are instructions are on how to set up your IMfree to interact wirelessly with iTunes. Note that these commands could also be sent via a cell phone or any other mobile device. The possibilities are enormous. This tutorial is meticulous and is intended to make sure that all of it will work properly. If it seems like novice material at times, I apologize. The result is well worth the effort.

1. Create two AIM screen names. If you already have two that is perfectly fine. Designate one to be the receiver on the host PC and one to be logged in on the IMfree.

2. Go to http://maximized.com/download/free➥ware/scriptsforitunes/setup.exe to download the iTunes scripts that will be executed remotely through AIM. Since the original Winamp plan needed a command line interface, I figured out that these scripts could be executed as well to control iTunes. The scripts were written in VB and are automatically installed in the iTunes directory with an exe file.

3. Download and install the Trillian software. Get a 15 day trial to test out the advanced functions that are needed in this test. Go to Trillian, Upgrade to Trillian Pro, and Request an Evaluation Version. Login with the password given through the email and reboot Trillian.

4. Launch Trillian Pro and go to Trillian, Trillian

Preferences, and click on Plugins. Click on AIM/ICQ and go to Trillian Preferences again and on the right hand side click on Add a New IM Connection. Configure all of your login information for the AIM screen name that will be receiving the data from the IMfree. Login with this screen name on Trillian. For further explanation later on, my fictitious screen name will be called ItunesRemote.

5. Now for the fun stuff. I must give credit to Jason over at www.teknikill.net/bbs/ for giving me the idea and the foundation for the rest of this article. His instructions worked when I tried them, so I am only adapting them a bit to match our iTunes experiment criteria.

6. Go to Trillian -} Trillian Preferences and then click on Advanced Preferences.

7. Click on Automation in the left hand menu.

8. Click Add -} Word Matching.

9. In the Add Word Match Entry box enter the word '"launch" in the word text box, check Match Whole Word and check Generate Event, then enter something for the event type (just use "launch" again).

10. Click on Add Event.

11. Next to Action Type change Sound to Execute Program. (You probably see where this is leading to by now. If not, keep reading anyway.)

12. Browse to the location of your iTunes exe file and select it as the program that you wish to execute. It will most likely be in "C:\ Program Files\ iTunes". Click Set Event.

13. This will take you back to the Match Word Entry menu. Make sure that everything is right and that the word is "launch". Also make sure that the entry type is called "launch". Click Save.

It's now time to cook the shish kabob. Login with your IMfree screen name and IM your other screen name (ItunesRemote) with just the word "launch". Voila, iTunes launches! If your firewall is blocking iTunes from launching, just check Remember This Setting and Allow if you run on Zonealarm. Do likewise if you have a different firewall. All that you need to do to play a song, skip a song, etc. is to repeat steps 6-13 by replacing the location of the iTunes exe file with one of the iTunes scripts that was installed originally. For instance, if you wanted to play a song you would have Trillian execute the script called Play in C:\ Program Files\ iTunes\ Scripts, if that's where you put it. Also, remember to type in the word that Trillian will match with the program as Play, so that when you send the message of Play to ItunesRemote, it will execute the script and play the song.

Trillian Pro does not seem to have a limit on the number of commands that it can execute on the host PC. I have about five commands running, including the ability to change the volume, all on my IMfree. The possibilities for this application are limitless. Any application or program for that matter can be launched or executed half a world away with a cell phone. The only setback is that Trillian Pro has a price tag of $25. At least test it out with the trial version and prepare to be amazed. The IMfree can be bought on eBay for about $10 and on Amazon for $30, making this wireless iTunes remote cost between $35-$55. Imagine queueing up the song "I'll Be Home For Christmas" on your PC in America while sitting in the Tokyo airport with nothing but your cell phone. Please, let the imagination run wild.

The Not-So-Great Firewall of China

by Tokachu
tokachu@gmail.com

When most people think of Internet censorship, they tend to think about China the most. While many other countries have some sort of state-controlled Internet policy, most people would refer to China because of the sheer size of the population and government. Ironically enough, the country with one of the largest Internet populations seemed to go for the lowest bidder when it came to Internet censorship devices, replacing quality control with frantic developers pressed for time.

No matter how strange that may be, it still does not justify a government which wants to keep full control over all media. Which is why I'll tell you, and hopefully a Chinese friend, how the "Great" firewall works and how to keep it from ruining your Internet.

How It Works

Unlike most other countries that simply block all TCP traffic or utilize a filtering HTTP proxy, China relies almost solely on special routers designed to censor based on raw TCP data instead of HTTP requests. The government of China relies on two main methods of censorship: flooding fake DNS requests and forging TCP connection resets.

DNS Poisoning

Very few domain names are actually "blocked" using this method. For a DNS poison to take place, there must be a request for a very, very, very naughty website (like minghui.org) placed. This keeps anyone from figuring out how to connect to, let alone down-

load content from, a forbidden host.

Here's how an uncensored DNS request would look like in China:

```
0.000000 192.168.1.2 -> 220.194.59.17
DNS Standard query A baidu.com
0.289817 220.194.59.17 -> 192.168.1.2
DNS Standard query response A
202.108.22.33 A 220.181.18.114
```

And here's how it would look if a domain were censored:

```
0.000000 192.168.1.2 -> 220.194.59.17 DNS
Standard query A minghui.org 0.288963
220.194.59.17 -> 192.168.1.2 DNS Standard
query response A 203.105.1.21 0.289482
220.194.59.17 -> 192.168.1.2 DNS Standard
query response A 203.105.1.21 0.289838
220.194.59.17 -> 192.168.1.2 DNS Standard
query response A 203.105.1.21 0.290374
220.194.59.17 -> 192.168.1.2 DNS Standard
query response A 203.105.1.21 0.290732
220.194.59.17 -> 192.168.1.2 DNS Standard
query response A 203.105.1.21 0.290757
192.168.1.2 -> 220.194.59.17 ICMP
Destination unreachable (Port unreachable)
0.291311 220.194.59.17 -> 192.168.1.2 DNS
Standard query response A 169.132.13.103
0.291337 192.168.1.2 -> 220.194.59.17 ICMP
Destination unreachable (Port unreachable)
```

The real reply never gets through because the router forges nearly a half dozen fake DNS replies, along with a few random ICMP messages, to whoever requests a "forbidden" website. This filter only works on UDP port 53 (DNS), which would theoretically make uncensored DNS requests possible if a sufficient number of DNS servers running on ports other than 53 existed.

You can tell if your packets are going through a Chinese router by one simple test. Try performing a DNS query to a remote machine in China. If it doesn't go through, try performing a DNS query for "minghui.org" on the same machine. If you get seemingly random responses, you're routing through China. If you want to determine which router is responsible for the censorship, run a traceroute and perform DNS requests on each hop, starting at the closest. When you get the fake DNS replies, you've found the offending router.

Forging TCP Resets

If a TCP connection is made from or to a computer in China, the packet data is checked for any "forbidden" words. If the data contains any of those words, the router forges a TCP RST (reset connection) packet. This also triggers a temporary block on TCP connections between those two specific computers. This makes it appear that the server has gone down temporarily.

The list of words not permitted to be used are encoded in GB2312 format, which ensures that businesses with websites in China will not be able to send any illegal content to computers in China (since GB2312 is a character set required to be supported by all applications in China). The filter works thusly:

If the word can be written in pure ASCII, look for the word in any mixture of lowercase and uppercase ASCII letters.

If the word must be written in any combination of CJK ideographs, look for the byte sequence in either raw or URL-encoded GB2312. Hexadecimal strings are also case-insensitive.

Problems

Nearly all the problems of China's firewalls stem from one problem with the routers: they all perform stateless packet inspection. It doesn't matter what protocol the packets are using, nor what computer a packet comes from. All the router is concerned with is finding packets and forging responses, not dropping content.

Unfortunately, that flaw puts the router owners and admins at an extreme disadvantage. Anybody can do a Google search for packet-forging software or libraries (such as libpcap) and whip up a script to flood Chinese routers with fake packets – and the routers will respond, no matter what. It wouldn't be difficult to set up a botnet with DNS request forgers that can send billions of fake DNS requests to various routers, and in return have the victim think China is attacking his or her server! It's also possible to forge a TCP data packet with fake source and destination addresses, which means that if you happened to know the IP addresses of two important diplomats, you could easily cut off their ability to communicate. Popular Chinese websites are just as vulnerable too; email systems could be cut off for hours at a time. The possibilities are endless. The TCP RST timer may be fairly short, but keep in mind that it only takes one fake packet to close a connection.

Getting Around It

The TCP Stack. One way to tell fake RST packets from real RST packets is to look at the time-to-live (TTL) parameter. Forged packets will always have higher TTLs than the real ones. Getting around this, however, would require that both parties have a stateful TTL comparison filter at the kernel level. That's no good.

You could, however, rewrite a TCP-based application to send "forbidden" words by using the TCP urgent flag (URG). This only requires that both parties have a modified application - no kernel tweaking necessary. A great example of a program that sends data like that is a proof-of-concept C program called "covertsession" (search for it on Packet Storm Security). It can bypass most stateful packet inspectors, so it easily gets around the stateless inspectors in China. This is probably the best way to modify instant messaging (such as QQ) and IRC applications, assuming one couldn't just use encryption on both ends.

HTTP Traffic. There's nothing really special about how the firewall treats HTTP traffic. Mind you that it only looks for certain strings, no matter where they are. But notice how I said it only uses the GB2312 character set: there's nothing stopping us from simply using UTF-8 instead. You can "switch" your websites from GB2312 to UTF-8 by simply running them through iconv. It's impossible for any UTF-8 sequence to match a GB2312 sequence, even by

accident, so you're partially assured good exposure (for a period of time).

Most China-based web hosts, such as Baidu and Yahoo! China, rely on the firewalls to block some content for them. Google China, however, is the one huge exception. Google's Chinese servers are located in the United States and their censorship is done entirely in-house. What does that mean? For one, we don't need to worry about text being sent in GB2312 format (Google insists on using UTF-8). We can also exploit a "feature" in Google's text engine that was overlooked during the Google China development.

Google doesn't compare strings in their text engine like most of us do. Instead of simply comparing bytes, Google considers some words and characters equal to other words and characters that wouldn't match with a byte comparison algorithm. The character equality is what we want to look at here: mainly, how Google considers "fullwidth" ASCII characters (wide, fixed-width characters mostly used in Japanese character sets) equal to their ASCII counterparts. If you were to search for "computers" using fullwidth characters, you'd get the same results as you would with a simple ASCII search (although some ads might not show up).

Now here's where the hack comes in: Google's censors don't look for those fullwidth characters. So, if we were to search Google China for "tiananmen square" using fullwidth characters, the results wouldn't be filtered (the connection may be reset from what Google sends). Luckily, this trick works for Google Images - meaning that it isn't too hard to get Google's cache of images normally unfindable in China!

Here's some sample code to generate fullwidth characters in a shell in Perl (assuming you've got Unicode support in your terminal):

```
#!/usr/bin/perl -w
# fw.pl - make text W-I-D-
E (convert ascii to fullwidth)
use encoding "UTF-8";
$input = $ARGV[0] or die("need
one argument for text");
foreach (split //, $input) { print
chr(0xFEE0 + ord($_)); }
## end script
```

Just type whatever search term you want, plug in the output to Google, and watch once-censored search results just show up!

Conclusion

Censorship isn't a profitable business. If China were to release an honest budget (and if people and corporations found out a huge percentage of their GDP was going towards censorship and propaganda instead of food and health care), China's economy would collapse in a matter of hours. Sadly, it isn't just Chinese citizens who believe the lies: corporations like Cisco and Google actually believe you can make money by keeping information from people. The sooner the Chinese people and their government realize this, the better.

(There are far too many people to thank - you know who you are.)

Hactivism in the Land Without a Server

by \ /indic8tr

A little while back I stumbled upon a link to the forums of the Korean Friendship Association (http://➥www.korea-dpr.com/cgi-bin/simpleforum.cgi). Naturally, I thought they needed to hear my opinion on the plight of the people of North Korea. Unfortunately, there is no obvious way of registering for a forum membership without joining their club, nor could I discover any less obvious means to gain access.

Not being content to walk away in total defeat, I decided to examine other parts of the site. After a little research, I discovered that this domain in fact houses the official website of the Democratic People's Republic of Korea. A whois search for the korea-dpr.➥com domain shows that the server is located in, of all places, Spain.

This seems counterintuitive at first glance. However, this makes perfect sense for a country where information is so tightly controlled that it is a capital crime to own a radio that is not hardwired to receive only the single government-approved station. That the DPRK cannot permit their own government's public website, their equivalent to whitehouse.gov, to be located on a server within its own borders flows naturally from this mindset. Clearly, North Korea isn't a place that is easily targeted by those who would seek to use online activism to further the free flow of knowledge. This is frustrating, because hactivism is one of the few nonviolent routes we have to bring the fight to those who would stifle learning and creativity both at home and abroad.

While we can't pick on Dear Leader directly, someone could hypothetically stick it to his fan club. Using techniques similar to the "Having Fun with Cookies" article in 23:3, a malicious user can use inline javascript in a browser's address bar to get free stuff courtesy of the Korean Friendship Association.

This will require the attacker to set up a throwaway PayPal account or a one-time use credit card. They would also need a little knowledge of Spanish. Don't worry, a hypothetical attacker wouldn't have to spend any real money for this to work.

The KFA online store is located at http://www.➥korea-dpr.com/catalog2/index.php. Our hypothetical angry activist first should choose something to buy, preferably something expensive. Then he or she would select the "Buy Now!" option, then go on to the checkout. There, the attacker would fill out the information form. If they want to actually receive the stuff and not get busted, they would probably want to use a P.O. box that can't be traced back to them, since most developed countries are still on reasonably good terms with Spain, if not the DPRK. Note that even if one selects payment in U.S. dollars, they will still be billed in euros. Hit continue twice to use the same P.O. box you submitted earlier for your shipping and billing addresses.

The hack is executed on the Order Confirmation form, and it is a simple one. The website uses a POST to send the price info to PayPal in the form of a javascript variable. The price of the fist item is stored in the variable document.forms[2].amount_1. If you purchased other items, they'll be stored in amount_2, amount_3, and so on.

Go to the address bar and enter the following:

```
javascript:void(document.forms[2].amount
➥_1.value="0.00");alert(document.forms
➥[2].amount_1.value)
```

The alert box isn't strictly necessary, but it is nice to know that the variable was successfully changed. If you bought more than one item, go through and repeat for amount_2, amount_3, and so forth as needed.

All that remains is to confirm your order in the Spanish language form (WTF?) and presto, free North Korean stuff. Maybe such a kick in the pocket book would help the membership of the KFA to see the *irony of running an e-commerce website on* behalf of a regime that would shoot its own citizens for using a computer or, up until recently, buying things.

K7: Free [for the taking] Voicemail

by noir
noir.na@gmail.com

K7.net is a site providing free, web-based voicemail and fax services. I'll be specifically addressing the voicemail service in this article, but I have no doubt that the following will apply to the fax services as well. I figured a free voicemail service with no hooks or hidden agendas, what's the harm in trying? This article details exactly the harm found. And for the record, I did email the company expressing my concerns and willingness to help, but shockingly I never heard back from them.

The basics of the service are very simple. You sign up for your free account, they assign you your own phone number and you can now receive voicemails from that number either in your email or by logging into the K7 site. You have the option to either let K7 pick a number for you or search to find a vanity number. When you register, the only information you have to provide is your email address, a four digit security code, how you found their service, and the specifics on how you want to receive your messages. This is when I first started questioning their security practices. Your pin must be four digits exactly and cannot start with a zero. With all 9000 possibilities this provides, somebody would be crazy to think they could have a script brute force an account. No matter, you'll see shortly that the strength of the pin doesn't matter. On to the good stuff.

Let's head on over to voicemail.k7.net to log in and start playing. After logging in, if you click on **Check Your Messages**, the URL looks something like this:

```
http://voicemail.k7.net/listen.asp?Phone
➥=YOURNUMBER&newSession=true&sOrder=
```

Now go ahead and delete your voicemail. k7.net cookie for this session. We certainly don't want the site to think you're trying to change your account when you're trying to change somebody else's. That could be disastrous. The next step is a bit advanced, so hopefully I don't lose any readers with its complexity. Change the phone number in the URL to the number for the account you're interested in. Everyone still with me? If you click on **Modify Settings** you'll be able to see the user information for whomever has that number. If all the fields on that page are blank it has either not been registered or it's not a number provided by K7. The use of this gaping security hole is clear. If you got a new email and wanted the voicemails sent there but you can't remember your PIN, now you can go in, update your email and change your PIN to something you won't forget so easily next time (you silly goose). Or perhaps you don't want "yourself" to know that you're accessing the account. You can just make sure the account is set to save messages to K7's site and just listen to them on there. I'm sure you can figure out the rest of the possibilities at this point.

I think it's also important to note that K7 is owned by a company who also provides other phone services, including 800 services for businesses. While the security on the other sites may vary, does the fruit fall that far from the tree?

Marketplace

For Sale

VENDING MACHINE JACKPOTTERS. Go to www.hackershomepage.com for EMP Devices, Lock Picks, Radar Jammers & Controversial Hacking Manuals. 407-965-5500

MAKE YOUR SOFTWARE OR WEBSITE USER FRIENDLY with Foxee, the friendly and interactive cartoon blue fox! Not everyone who will navigate your website or software application will be an expert hacker, and some users will need a little help! Foxee is a hand-animated Microsoft Agent character that will accept input through voice commands, text boxes, or a mouse, and interact with your users through text, animated gestures, and even digital speech to help guide them through your software with ease! Foxee supports 10 spoken languages and 31 written languages. She can be added to your software through C++, VB6, all .Net languages, VBScript, JavaScript, and many others! Natively compatible with Microsoft Internet Explorer and can work with Mozilla Firefox when used with a free plug-in. See a free demonstration and purchasing information at www.foxee.net!

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. See why everyone at HOPE Number Six loved it. Turning off TVs really is fun. $20.00 each. www.TVBGone.com

JUST RELEASED! Feeling tired during those late night hacking sessions? Need a boost? If you answered yes, then you need to reenergize with the totally new *Hack Music Volume 1* CD. The CD is crammed with high energy hack music to get you back on track. Order today by sending your name, address, city, state, and zip along with $15 to: Doug Talley, 1234 Birchwood Drive, Monmouth, IL 61462. This CD was assembled solely for the readers of *2600* and is not available anywhere else!

NET DETECTIVE. Whether you're just curious, trying to locate or find out about people for personal or business reasons, or you're looking for people you've fallen out of touch with, Net Detective makes it all possible! Net Detective is used worldwide by private investigators and detectives, as well as everyday people who use it to find lost relatives, old high school and army buddies, deadbeat parents, lost loves, people that owe them money, and just plain old snooping around. Visit us today at www.netdetective.org.uk.

JEAH.NET UNIX SHELLS SINCE 1999 - JEAH's FreeBSD shell accounts continue to be the choice for performance-driven uptimes and a huge list of virtual hosts. JEAH accounts let you store data, use IRC, SSH, and email with complete privacy and security. JEAH also offers fast, stable virtual web hosting and complete domain registration solutions - including registration with masked WHOIS info. Mention *2600* and receive setup fees waived! Join the JEAH.NET institution!

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a supplier of Network Security and Internet Privacy products. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers, IP access devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you... No surprises! Buy with confidence! Security and Privacy is our business! Visit us at http://www.OvationTechnology.com/store.htm.

PHONE HOME. Tiny, sub-miniature, 7/10 ounce, programmable/reprogrammable touch-tone, multi-frequency (DTMF) dialer which can store up to 15 touch-tone digits. Unit is held against the telephone receiver's microphone for dialing. Press "HOME" to automatically dial the stored digits which can then be heard through the ultra miniature speaker. Ideal for E.T.'s, children, Alzheimer victims, lost dogs/chimps, significant others, hackers, and computer wizards. Give one to a boy/girl friend or to that potential "someone" you meet at a party, the supermarket, school, or the mall; with your pre-programmed telephone number, he/she will always be able to call you! Also, ideal if you don't want to "disclose" your telephone number but want someone to be able to call you locally or long distance by telephone. Key ring/clip. Limited quantity available. Money order only. $24.95 + $3.00 S/H. Mail order to: PHONE HOME, Nimrod Division, 331 N. New Ballas Road, Box 410802, CRC, Missouri 63141.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? Read the all-new *Access All Areas*, a guidebook to the art of urban exploration, from the author of *Infiltration* zine. Send $20 postpaid in the US or Canada, or $25 overseas, to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada, or order online at www.infiltration.org.

ENHANCE OR BUILD YOUR LIBRARY with any of the following CD ROMS: Hack Attacks Testing, Computer Forensics, Master Hacker, Web Spy 2001, Hackers' Handbook, Troubleshooting & Diagnostics 98, PC Troubleshooter 2000, Forbidden Subjects 3, Hackers Toolkit 2.0, Steal This CD, Hacks & Cracks, Hackerz Kronicklez, Elite Hackers Toolkit 1, Forbidden Knowledge 2, Troubleshooting & Diagnostics 2002, Police Call Frequency Guide 2nd Edition, Computer Toybox, Answering Machine 2000, Hackers Encyclopedia 3, Maximum Security 3rd Edition, Network Utilities 2001, Screensavers 2002, Engineering 2000, Anti-Hacker Toolkit 2nd Edition & PC Hardware. Send name, address, city, state, zip, email address (for updates only) and items ordered, along with a cashier's check or money order in the amount of $20 for each item to: Doug Talley, 1234 Birchwood Drive, Monmouth, IL 61462.

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at *http://store.2600.com*. (VHS copies of the film still available for $15.)

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a *2600* member by dangling your keychain and saying nothing. Cover one hole and get exactly *2600 hz*, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $79.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

PHRAINE. The technology without the noise quarterly would like to thank the *2600* readers who have also become new subscribers and encourages those who have not ACK their need for diverse computer information in conjunction with that of *2600* to dedicate some packets and become a subscriber today! Visit us at our new domain www.pearlyfreepress.com/phraine.

JINX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v3no2" and get 10% off of your order.

LEARN LOCK PICKING. It's EASY with our book and new video. The 2nd edition book adds lots more interesting material and illustrations while the video is filled with computer graphic cutaway views. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks for the book or video to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your *2600* reader price discount.

CABLE TV DESCRAMBLERS. New. Each $55 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescramblerguy@yahoo.com.

Wanted

HAVE KNOWLEDGE OF SECURITY BREACHES at your bank? Heard rumors of cracked customer databases? Know there are unaddressed vulnerabilities in a retailer's credit card network, but its management doesn't know or care? We want your tips. We are a business newsletter focusing on security issues in the financial industry: IT security, privacy, regulatory compliance, identity-theft and fraud, money-laundering. Wherever criminal activity meets banks, we are there. You can remain anonymous. (Note: we will not print rumors circulated by one person or group without obtaining supporting evidence or corroboration from other parties.) Contact banksecuritynews@yahoo.com or call 212-564-8972, ext. 102.

Services

HACKER TOOLS TREASURE BOX! You get over 630 links to key resources, plus our proven methods for rooting out the hard-

to-find tools, instantly! Use these links and methods to build your own customized hacker (AHEM, network security) tool kit. http://wealthfunnel.com/securitybook

ADVANCED TECHNICAL SOLUTIONS. #422 - 1755 Robson Street, Vancouver, B.C. Canada V6G 3B7. Ph: (604) 928-0555. Electronic countermeasures - find out who is secretly videotaping you or bugging your car or office. "State of the Art" detection equipment utilized.

FREERETIREDSTUFF.COM - Donate or request free outdated tech products - in exchange for some good karma - by keeping usable unwanted tech items out of your neighborhood landfill. The FREE and easy text and photo classified ad website is designed to find local people in your area willing to pick up your unwanted tech products or anything else you have to donate. Thank you for helping us spread the word about your new global recycling resource by distributing this ad to free classified advertising sites and newsgroups globally. www.FreeRetiredStuff.com

SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information. I am an aggressive criminal defense lawyer specializing in the following types of cases: unauthorized access, theft of trade secrets, identity theft, and trademark and copyright infringement. Contact Omar Figueroa, Esq. at (415) 986-5591, at omar@stanfordalumni.org, or at 506 Broadway, San Francisco, CA 94133-4507. Graduate of Yale College and Stanford Law School. Complimentary case consultation for 2600 readers. All consultations are strictly confidential and protected by the attorney-client privilege.

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted at Chicago Equinix with Juniper Filtered DoS Protection. Multiple FreeBSD servers at P4 2.4 ghz. Affordable pricing from $5/month with a money back guarantee. Lifetime 26% discount for 2600 readers. Coupon code: Save2600. http://www.reverse.net

ANTI-CENSORSHIP LINUX HOSTING. Kaleton Internet provides affordable web hosting, email accounts, and domain registrations based on dual processor P4 2.4 GHz Linux servers. Our hosting plans start from only $8.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. You can now choose between the USA, Singapore, and other offshore locations to avoid censorship and guarantee free speech. We respect your privacy. Payment can be by E-Gold, PayPal, credit card, bank transfer, or Western Union. See www.kaleton.com for details.

ARE YOU TIRED of receiving piles of credit card offers and other postal spam? You can't just throw them in the trash or recycle them as someone could get a hold of them and use them to steal your identity. You can't just let them pile up on your kitchen table. So instead you have to be bothered with shredding and disposing of them. Well, not anymore. OperationMailBack.com has a free solution for you. All costs of disposal including delivery will be paid by the company responsible for sending the stuff to you. Stop wasting your valuable time dealing with messes other people are responsible for creating. Check out our newly redesigned website for complete information and take back your mailbox.

BEEN ARRESTED FOR A COMPUTER OR TECHNOLOGY RELATED CRIME? Have an idea, invention, or business you want to buy, sell, protect, or market? Wish your attorney actually understood you when you speak? The Law Office of Michael B. Green, Esq. is the solution to your 21st century legal problems. Former SysOp and member of many private BBS's since 1981 now available to directly represent you or bridge the communications gap and assist your current legal counsel. Extremely detailed knowledge regarding criminal and civil liability for computer and technology related actions (18 U.S.C. 1028, 1029, 1030, 1031, 1341, 1342, 1343, 2511, 2512, ECPA, DMCA, 1996 Telecom Act, etc.), domain name disputes, intellectual property matters such as copyrights, trademarks, licenses, and acquisitions as well as general business and corporate law. Over eleven years experience as in-house legal counsel to a computer consulting business as well as an over 20 year background in computer, telecommunications, and technology matters. Published law review articles, contributed to nationally published books, and submitted briefs to the United States Supreme Court on Internet and technology related issues. Admitted to the U.S. Supreme Court, 2nd Circuit Court of Appeals, and all New York State courts and familiar with other jurisdictions as well. Many attorneys will take your case without any consideration of our culture and will see you merely as a source of fees or worse, with ill-conceived prejudices. My office understands our culture, is sympathetic to your situation, and will treat you with the respect and understanding you deserve. No fee for the initial and confidential consultation and, if for any reason we cannot help you, we will even try to find someone else who can at no charge. So you have nothing to lose and perhaps everything to gain by contacting us first. Visit us at: http://www.computerney.com or call 516-9WE-HELP (516-993-4357).

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Shows from 1988-2005 are now available in DVD-R format for $30! Or subscribe to the new high quality audio service for only $50. Each month you'll get a newly released year of Off The Hook in broadcast quality (far better than previous online releases). Send check or money order to 2600, PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

PHONE PHUN. http://phonephun.us. Blog devoted to interesting phone numbers. Share your finds!

DO YOU WANT ANOTHER PRINTED MAGAZINE that complements 2600 with even more hacking information? Binary Revolution is a magazine from the Digital Dawg Pound about hacking and technology. Specifically, we look at underground topics of technology including: Hacking, Phreaking, Security, Urban Exploration, Digital Rights, and more. For more information, or to order your printed copy online, visit us at http://www.binrev.com/ where you will also find instructions on mail orders. Welcome to the revolution!

CHRISTIAN HACKERS' ASSOCIATION: Check out the web page http://www.christianhacker.org for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.

Personals

SEEKING NON-STAGNANT MINDS for mutual illumination/exchange of thoughts and ideas. Three years left on my sentence and even with all my coaching the walls still can't carry a decent conversation. Interests include cryptography, security, conspiracy theories, martial arts, and anything computer related. All letters replied to. Max Rider, SBI#00383681 D.C.C., 1181 Paddock Rd., Smyrna, DE 19977.

IN SEARCH OF FRIENDS/CONTACTS: Railroaded by lying evidence-burying FBI agents and U.S. Postal Inspectors for crime I didn't commit. In court I had a snowball's chance in hell. Unless I outsmart the government by exhuming the exculpatory treasure trove of my innocence, I'm hopelessly dungeoned for the duration. There's only a little gleam of time between two eternities. I refuse to return to forever without a fight. Will answer all. W. Wentworth Foster #21181, Southeast Correction Center, 300 East Pedro Simmons Drive, Charleston, MO 63834.

PRISONER SEEKS FRIENDS to help with book review lookups on Amazon by keywords. Com Sci major, thirsty to catch up to the real world before my reentry. I have my own funds to buy books. I only need reviews. Or... I'm MUD/MMORPG savy in C++/Python/PHP/MySQL, and I'm seeking players and programmers for better idea on "what's out there." Please help. Ken Roberts J60962, CSTAF-A2-244 UP, PO Box 5248, Corcoran, CA 93212.

OFFLINE OUTLAW IN TEXAS is looking for any books Unix/Llinux I can get my hands on. Also very interested in privacy in all areas. If you can point me in the right direction or feel like teaching an old dog some new tricks, drop me a line. I'll answer all letters. Props to those who already have, you know who you are. William Lindley 822934, 1300 FM 655, Rosharon, TX 77583-8604.

IN SEARCH OF NEW CONTACTS every day. I have a lot of time to pass and am always up for a good discussion. Joint source audit anyone? Of course it'll have to be on paper. Interests not limited to: low-level OS coding, embedded systems, crypto, radiotelecom, and conspiracy theory. Will reply to all. Brian Salcedo #32130-039, FCI McKean, P.O. Box 8000, Bradford, PA 16701.

STILL IN THE JOINT. Only a year or so left. Known as Alphabits, busted for hacking banks and lots of unauthorized wire transfers. I'm looking to hear from anyone in the free world. Very interested in any ideas regarding future employment. Will respond to all. Jeremy Cushing #J51130, Centinela State Prison, PO Box 921, Imperial, CA 92251-0921.

CONVICTED COMPUTER CRIMINAL in federal prison doing research on Asperger Syndrome prevalence in prison. Please write: Paul Cuni 15287-014, Box 7001, Taft, CA 93268.

STORMBRINGER'S 411: Am not getting a fair shake in court without an attorney, so it's 15 more years to pull. Need a coder for a web GUI for a shortwave/scanner (Icom PCR-1000) that I donated to a shortwave station and some other interesting stuff. Would love to talk shop with people on radio, data over radio, and ham radio. Will respond to all letters technical or not. W.K. Smith, 44684-083, FCI Cumberland, PO Box 1000, Cumberland, MD 21501-1000. Web: www.stormbringer.tv. Link to it!

ONLY SUBSCRIBERS CAN ADVERTISE IN 2600! Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. **Deadline for Spring issue: 3/1/07.**

قاحمجنم

What does it mean? How do all of those things tie together? Come up with the best way of phrasing it and win a prize! Email puzzle@2600.com

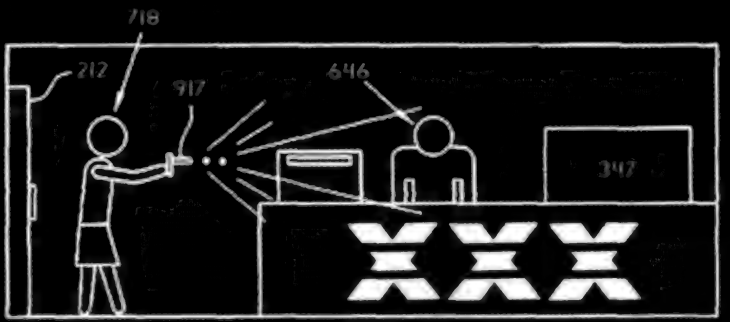


FIG. 4A

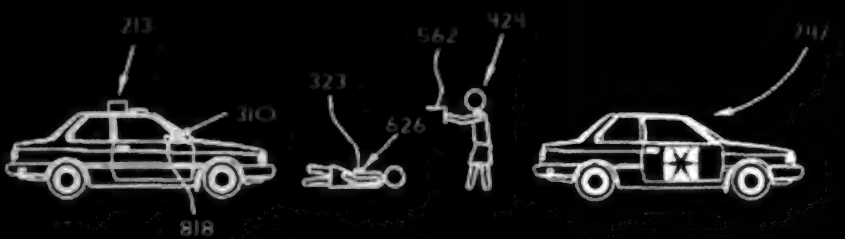


FIG. 4B

Answer choice for Autumn 2006 puzzle:

"Are Pac-Man, Apple, Microsoft, and Dual-Core grain silos as American as Pi? No!"

-- Mister Ule, 20500

NEW PRICES

So how does all this affect you? Simple. It won't affect you at all if you're a subscriber. If you buy us at a newsstand in the United States, you'll pay 75 cents more. If you buy us at a newsstand in Canada, you'll pay a dollar less. And if you're somewhere else, we honestly don't know.

As this is our first price change on the newsstand in more than three years and only the second since 1999, it's actually a bargain considering how much the cost of everything has gone up in that period and the fact that we've added lots of pages over the years. But if you wish to *really* cling to the past, consider that our subscription price has not gone up in over 15 years! How insane is *that?*

All in all, we believe it's still a pretty good deal, regardless of how you choose to buy our zine. Remember that we survive solely on subscriber support. If we had advertising we could probably give the thing away for free. But then we just wouldn't be the same and would probably be unable to print the kinds of things we enjoy printing.

If you found us in a bookstore or at a newsstand, you're probably aware that most of the magazines surrounding us are nothing like *2600.* By keeping our sales strong, you're voicing support for something different and hopefully that will enable other alternatives to be considered by distributors and bookstores as well. And this is how the general public is reached. Despite all of the TV channels, audio devices, and Internet blogs we're constantly bombarded with, they are just no substitute for books and magazines. We hear comments like this more than ever these days.

So here's the deal. If you buy the copy you're holding in your hand at a store, there's no need to read further (unless you want some back issues). If you want to subscribe, it's $20 for the U.S. and Canada, $30 elsewhere. Back issues are $5 each ($6.50 overseas) except for the most recent one which is $5.50 ($7.00 overseas). Plus there are all sorts of bulk discounts available at our online store located at http://store.2600.com.
The address to send physical subscription and back issue requests is:

2600
PO Box 752
Middle Island, NY 11953 USA

(Don't worry, it comes in an envelope that doesn't have our name on it, just our return address. We're aware of evil parents, spouses, bosses, and prison guards who are watching you.)

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Melbourne: Caffeine at ReVault Bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm.

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St. at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall. 6 pm.

British Columbia

Vancouver: Lupo Caffe & Bar, 1014 West Georgia St.

Victoria: QV Bakery and Cafe, 1701 Government St.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Ground Zero Networks Internet Cafe, 720 Main St. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.

Guelph: William's Coffee Pub, 492 Edinbourgh Road South. 7 pm.

Ottawa: World Exchange Plaza, 111 Albert St., second floor. 6:30 pm.

Toronto: College Park Food Court, across from the Taco Bell.

Waterloo: William's Coffee Pub, 170 University Ave. West. 7 pm.

Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm.

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm.

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). 7 pm. Payphone: (01273) 606674.

Exeter: At the payphones, Bedford Square. 7 pm.

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm.

Manchester: The Green Room on Whitworth St. 7 pm.

Norwich: Borders entrance to Chapelfield Mall. 6 pm.

Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Grenoble: Eve, campus of St. Martin d'Heres. 6 pm.

Paris: Place de la Republique, near the (empty) fountain. 6:30 pm.

Rennes: In front of the store "Blue Box" close to Place de la Republique. 8 pm.

GREECE

Athens: Outside the bookstore Papaswtiriou on the corner of Patision and Stoumari. 7 pm.

IRELAND

Dublin: At the phone booths on Wicklow St. beside Tower Records. 7 pm.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.

Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.

Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm.

Trondheim: Rick's Cafe in Nordregate. 6 pm.

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm.

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN

Gothenburg: 2nd floor in Burger King at Avenyn. 6 pm.

Stockholm: Outside Lava.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.

Huntsville: Stanlieo's Sub Villa on Jordan Lane.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Peter Piper Pizza, 3945 E. Thomas Rd.

Tucson: Borders in the Park Mall. 7 pm.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: London Bridge Pub, 2 Wharf II.

Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive. 8 pm.

Sacramento: Round Table Pizza at 127 K St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806. 5:30 pm.

San Jose: Outside the cafe at the MLK Library at 4th and E. San Fernando. 6 pm.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.

Denver: Borders Cafe, Parker and Arapahoe.

District of Columbia

Arlington: Pentagon City Mall in the food court (near Au Bon Pain). 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm.

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm.

Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.

Pocatello: College Market, 604 South 8th St.

Illinois

Chicago: Neighborhood Boys and Girls Club, 2501 W. Irving Park Rd. 7 pm.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.

Indianapolis: Corner Coffee, SW corner of 11th and Alabama.

South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Wichita: Riverside Park, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's. 6 pm.

New Orleans: Z'otz Coffee House uptown at 8210 Oak Street. 6 pm.

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows. 6 pm.

Marlborough: Solomon Park Mall food court.

Michigan

Ann Arbor: The Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.

St. Louis: Galleria Food Court.

Springfield: Borders Books and Music coffeeshop, 3300 South Glenstone Ave., one block south of Battlefield Mall. 5:30 pm.

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: Coffee Bean Tea Leaf coffee shop, 4550 S. Maryland Pkwy. 7 pm.

New Mexico

Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. Payphones: 505-843-9033, 505-843-9034. 5:30 pm.

New York

New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

North Carolina

Charlotte: South Park Mall food court. 7 pm.

Raleigh: Royal Bean coffee shop on Hillsboro Street (next to the Playmakers Sports Bar and across from Meredith College).

North Dakota

Fargo: West Acres Mall food court by the Taco John's.

Ohio

Cincinnati: The Brew House, 1047 East McMillan. 7 pm.

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

Columbus: Convention center on street level around the corner from the food court.

Dayton: TGI Friday's off 725 by the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St. and Penn.

Tulsa: Promenade Mall food court.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm.

Pennsylvania

Allentown: Panera Bread, 3100 West Tilghman St. 8 pm.

Philadelphia: 30th St. Station, southeast food court near mini post office.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Atlanta Bread Co., 4770 Poplar Ave. 6 pm.

Nashville: J-J's Market, 1912 Broadway. 6 pm.

Texas

Austin: Spider House Cafe, 2908 Fruth St. 7 pm.

Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.

San Antonio: North Star Mall food court. 6 pm.

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm.

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge. Payphone: (608) 251-9909.

Milwaukee: The Node, 1504 E. North Ave.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time.

To start a meeting in your city, send email to meetings@2600.com.

More Western Hemisphere Phones

Dominican Republic. Found outside of **Dajabon.** It's debatable whether that dish and its solar panel, not to mention the huge conduit, are all there for this one little payphone, which seems to have had all its coin mechanisms removed.

Photo by Alex

Cuba. Two very different ETECSA models. This is part of the government owned communications service. The drab phone on the left takes coins, the bright and cheerful looking one on the right takes cards. Found in Veradero.

Photo by Alan Prusila

Visit **http://www.2600.com/phones/** to see even more foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photo

Here's a "glitch" that happened at the Barnes & Noble in Easton, Pennsylvania and captured by **l33tphreak** and **smoke**. Further proof that their scanning system doesn't always work. The cashier was overheard saying to all of the other clerks gathered round, "And it's a hacker magazine too."

Let's hope the cars don't also run on Windows.
This little crash was caught by **Brandon Freeman** on his way to work in Atlanta.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to articles@2600.com or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free two-year subscription (or back issues) and a 2600 sweatshirt (or two t-shirts).